# Vulnerability Prioritization Report

Findings from one Greenbone / OpenVAS export, grouped into the priority bands below.

| Generated | Scan date |
|---|---|
| 2026-09-13T18:36:00Z | 2026-09-05T00:09:57 |

Assessment

Assessment type: Automated network vulnerability assessment (Greenbone / OpenVAS, credential status not established), prioritized against CISA KEV exploitation data, with EPSS exploit-likelihood data reported alongside.

| Report ID | Confidentiality |
|---|---|
| 20260913T183600Z | Confidential — contains sensitive security information |

> **Report status: No exploitation intelligence**
> **This export carries no structured CVE references, so none of the 494 validated findings could be checked against CISA KEV or EPSS exploitation data. Findings are ranked by severity and CVSS only; the absence of a KEV match here reflects that no check was possible, not a clean result.**

| 459 | 494 | 1 |
|---|---|---|
| Distinct issues | Raw scan occurrences (incl. per-port duplicates) | Host scanned |

## Executive summary

The scan reports findings, but CVE-based exploitation assessment is unavailable because no retained finding carries a CVE.

Recommended priority action (A2): Version upgrade for 1 asset across 17 findings. Highest priority covered: Band 5 — no cve, non-trivial severity.

**Business impact themes**

- Unpatched software can leave known weaknesses available to attackers.
- Security-control gaps can leave exposed services or access paths insufficiently protected.
- Weak certificate or cryptographic settings can reduce confidentiality or trust in affected services.
- Some findings still require manual review before a safe fix can be selected.

### Assessment basis

No validated finding among the 459 distinct issues carries a CVE, so KEV and EPSS scored nothing. Findings are ranked by severity and CVSS below.

How far this scan could see: credential coverage is unknown. Undetected issues may remain, and conditions may have changed since the scan. These results do not establish the absence of vulnerabilities.

No quality-of-detection filter was applied (minimum quality-of-detection: 0). This describes the QoD threshold only; it does not establish that the export contains the full scan.

> Threat-exploitation status was not assessed because no validated finding carried a CVE for KEV or EPSS lookup.

308 remediation actions address 356 of 369 prioritized findings. 24 further actions appear under lower-priority and informational items.

- Authorize a re-scan with working credentials and a current signature feed to verify current coverage and findings. A low reported count is not evidence that few vulnerabilities exist.
- Authorize the remediation work below: 369 prioritized findings are covered by 308 actions.

Next step: agree the actions above, then re-scan to confirm both the fixes and what this scan could not see.

## Scope, scan quality & data quality

Band distribution

| Band | Description | Criteria | Issues |
|---|---|---|---|
| Band 1 | KEV + ransomware | in CISA KEV, with CISA-recorded use in known ransomware campaigns | 0 |
| Band 2 | KEV | in CISA KEV (CISA records these CVEs as known to have been exploited) | 0 |
| Band 3 | urgent CVSS, no KEV match | has a CVE with no KEV match in the catalog snapshot used, and CVSS at or above the urgent threshold of 9.0 | 0 |
| Band 4 | has CVE, non-trivial severity | has a CVE with no KEV match in the catalog snapshot used, below the urgent CVSS threshold, at a severity rating of 2 or above | 0 |
| Band 5 | no CVE, non-trivial severity | no CVE, but a severity rating of 2 or above | 369 |
| Band 6 | low or informational | any finding the bands above do not match | 90 |

| | |
|---|---|
| Scanner | Greenbone AG / Greenbone Community Feed |
| Scanner version | 23.50.20 |
| Policy | Unknown |
| Plugin feed date | 2026-09-04 |
| Scan window start | 2026-09-05T00:09:57 |
| Scan window end | 2026-09-05T00:39:01 |
| Credentialed | Unknown |
| Targets | Unknown |
| Quality-of-detection filter | No QoD filter (min_qod=0); other export filters may apply |

This export does not record a failed authenticated-checks attempt for any protocol this report checks. That is not evidence credentialed access succeeded -- this report does not infer a successful login from a scanner signal alone, so credential coverage for this scan is Unknown.

| | | | |
|---|---|---|---|
| **1**<br>Host scanned | **Unknown**<br>Credential coverage | **Unknown**<br>Hosts where patch assessment failed | **0**<br>Hosts missing a hostname |
| **0**<br>Hosts missing OS detail | **494**<br>Retained occurrences missing a CVE | **0**<br>Retained occurrences missing CVSS | **101**<br>Retained occurrences with no actionable solution (no text, or a placeholder such as "n/a") |
| **91**<br>Retained occurrences at informational severity | **0**<br>Findings excluded by the scanner's quality-of-detection filter | | |

Enrichment source: a non-default KEV catalog source (not confirmed to be CISA's published catalog) (retrieved 2026-09-13).

The scanner stated a quality-of-detection value for 494 of the 494 validated findings; the lowest among them was 30. Quality of detection is the scanner's own confidence that a finding is genuine, not a measure of severity.

What this scan cannot establish:

- Asset business criticality, ownership, and environment (production vs. development) — a vulnerability-scanner export carries no client-context fields for these.
- Internet exposure and data sensitivity per asset.
- Whether a finding has actually been exploited in this environment — only catalog-level exploitation evidence (CISA KEV) is available, which records exploitation elsewhere, not here.
- Configured scan exclusions and per-host scan timeouts — this report does not extract them from any export.
- Remediation SLA policy, ticketing state, or ownership/workflow assignment.

## Prioritized remediation plan

> EPSS estimates the likelihood of exploitation in roughly the next 30 days. It complements CISA KEV and CVSS and replaces neither: KEV records past exploitation, CVSS states technical severity, and EPSS estimates near-term exploitation probability.

a deterministic synthetic EPSS feed generated by tools/synthetic_epss_feed.py (not real EPSS data), retrieved 2026-09-13, model score date 2026-08-30.

Remediation actions are numbered A1, A2, … in a fixed order set once, when the plan was built -- not the order they appear on this page. The actions below appear in priority order; the no-scanner-supplied-solution bucket and any action covering only the lowest band appear afterward, under whatever number each was already assigned. Finding numbers (#1, #2, …) in the top urgent findings table and the technical appendix are a separate sequence; the two are not related.

## A2 Version upgrade on 1 asset — resolves 17 instances across 17 findings

Update to version 5.2.15 or later.

> Affected service: 80/tcp.

> This action consolidates 17 findings in the same release line with scanner-stated minimums 5.2.5, 5.2.6, 5.2.7, 5.2.8, 5.2.9, 5.2.10, 5.2.11, 5.2.12, 5.2.13, 5.2.14, 5.2.15. The highest stated minimum, 5.2.15, is shown above; the covered findings remain listed in the technical appendix.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): PHP 5.2.15 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A2. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Re-run the scan after the change and confirm the related scanner checks no longer report on the affected asset. The full check inventory appears in the scanner validation appendix. |

## A3 Version upgrade on 1 asset — resolves 10 instances across 10 findings

Update to version 2.4.66 or later.

> Affected service: 80/tcp.

> This action consolidates 10 findings in the same release line with scanner-stated minimums 2.4.49, 2.4.52, 2.4.53, 2.4.54, 2.4.55, 2.4.58, 2.4.59, 2.4.60, 2.4.64, 2.4.66. The highest stated minimum, 2.4.66, is shown above; the covered findings remain listed in the technical appendix.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): Apache HTTP Server 2.4.66 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A3. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugins 1.3.6.1.4.1.25623.1.0.100272, 1.3.6.1.4.1.25623.1.0.113837, 1.3.6.1.4.1.25623.1.0.114682, 1.3.6.1.4.1.25623.1.0.117856, 1.3.6.1.4.1.25623.1.0.125564, 1.3.6.1.4.1.25623.1.0.146725, 1.3.6.1.4.1.25623.1.0.148252, 1.3.6.1.4.1.25623.1.0.149152, 1.3.6.1.4.1.25623.1.0.152039, 1.3.6.1.4.1.25623.1.0.154909 after the change; they should stop reporting on the affected asset. |

## A4 Version upgrade on 1 asset — resolves 9 instances across 9 findings

Update to version 5.3.9 or later.

> Affected service: 80/tcp.

> This action consolidates 9 findings in the same release line with scanner-stated minimums 5.3.3, 5.3.4, 5.3.6, 5.3.7, 5.3.9. The highest stated minimum, 5.3.9, is shown above; the covered findings remain listed in the technical appendix.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): PHP 5.3.9 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A4. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugins 1.3.6.1.4.1.25623.1.0.100695, 1.3.6.1.4.1.25623.1.0.100901, 1.3.6.1.4.1.25623.1.0.103113, 1.3.6.1.4.1.25623.1.0.103229, 1.3.6.1.4.1.25623.1.0.103464, 1.3.6.1.4.1.25623.1.0.108869, 1.3.6.1.4.1.25623.1.0.108870, 1.3.6.1.4.1.25623.1.0.801585, 1.3.6.1.4.1.25623.1.0.902356 after the change; they should stop reporting on the affected asset. |

## A5 Version upgrade on 1 asset — resolves 6 instances across 6 findings

Update to version 5.6.31 or later.

> Affected service: 80/tcp.

> This action consolidates 6 findings in the same release line with scanner-stated minimums 5.6.0, 5.6.5, 5.6.7, 5.6.12, 5.6.26, 5.6.31. The highest stated minimum, 5.6.31, is shown above; the covered findings remain listed in the technical appendix.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): PHP 5.6.31 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A5. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugins 1.3.6.1.4.1.25623.1.0.805413, 1.3.6.1.4.1.25623.1.0.808611, 1.3.6.1.4.1.25623.1.0.808669, 1.3.6.1.4.1.25623.1.0.808673, 1.3.6.1.4.1.25623.1.0.809321, 1.3.6.1.4.1.25623.1.0.811490 after the change; they should stop reporting on the affected asset. |

## A6 Version upgrade on 1 asset — resolves 3 instances across 3 findings

Update to version 7.2.29 or later.

> Affected service: 80/tcp.

> This action consolidates 3 findings in the same release line with scanner-stated minimums 7.2.26, 7.2.28, 7.2.29. The highest stated minimum, 7.2.29, is shown above; the covered findings remain listed in the technical appendix.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): PHP 7.2.29 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A6. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugins 1.3.6.1.4.1.25623.1.0.143276, 1.3.6.1.4.1.25623.1.0.143541, 1.3.6.1.4.1.25623.1.0.143615 after the change; they should stop reporting on the affected asset. |

## A7 Version upgrade on 1 asset — resolves 3 instances across 3 findings

Update to version 4.9.2 or later.

> Affected service: 80/tcp.

> This action consolidates 3 findings in the same release line with scanner-stated minimums 4.9.0, 4.9.1, 4.9.2. The highest stated minimum, 4.9.2, is shown above; the covered findings remain listed in the technical appendix.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): phpMyAdmin 4.9.2 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A7. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugins 1.3.6.1.4.1.25623.1.0.142499, 1.3.6.1.4.1.25623.1.0.142897, 1.3.6.1.4.1.25623.1.0.143167 after the change; they should stop reporting on the affected asset. |

## A8 Version upgrade on 1 asset — resolves 3 instances across 3 findings

Update to version 1.3.2rc3 or later.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A8. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugins 1.3.6.1.4.1.25623.1.0.801640, 1.3.6.1.4.1.25623.1.0.900133, 1.3.6.1.4.1.25623.1.0.900507 after the change; they should stop reporting on the affected asset. |

## A9 Version upgrade on 1 asset — resolves 2 instances across 2 findings

Update to version 2.2.22 or later.

> Affected service: 80/tcp.

> This action consolidates 2 findings in the same release line with scanner-stated minimums 2.2.15, 2.2.22. The highest stated minimum, 2.2.22, is shown above; the covered findings remain listed in the technical appendix.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): Apache HTTP Server 2.2.22 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A9. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugins 1.3.6.1.4.1.25623.1.0.100514, 1.3.6.1.4.1.25623.1.0.147057 after the change; they should stop reporting on the affected asset. |

## A10 Version upgrade on 1 asset — resolves 2 instances across 2 findings

Update to version 1.9.0 or later.

> Affected service: 80/tcp.

> This action consolidates 2 findings in the same release line with scanner-stated minimums 1.9.0. The highest stated minimum, 1.9.0, is shown above; the covered findings remain listed in the technical appendix.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): jQuery 1.9.0 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A10. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugins 1.3.6.1.4.1.25623.1.0.141636, 1.3.6.1.4.1.25623.1.0.143968 after the change; they should stop reporting on the affected asset. |

## A11 Version upgrade on 1 asset — resolves 2 instances across 2 findings

Update to version 3.5.0 or later.

> Affected service: 80/tcp.

> This action consolidates 2 findings in the same release line with scanner-stated minimums 3.5.0. The highest stated minimum, 3.5.0, is shown above; the covered findings remain listed in the technical appendix.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): jQuery 3.5.0 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A11. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugins 1.3.6.1.4.1.25623.1.0.143812, 1.3.6.1.4.1.25623.1.0.143813 after the change; they should stop reporting on the affected asset. |

## A12 Version upgrade on 1 asset — resolves 2 instances across 2 findings

Update to version 3.0.32 or later.

> Affected service: 445/tcp.

> This action consolidates 2 findings in the same release line with scanner-stated minimums 3.0.24, 3.0.32. The highest stated minimum, 3.0.32, is shown above; the covered findings remain listed in the technical appendix.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): Samba 3.0.32 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugins 1.3.6.1.4.1.25623.1.0.150723, 1.3.6.1.4.1.25623.1.0.800711 after the change; they should stop reporting on the affected asset. |

## A13 Configuration change on 1 asset — resolves 2 instances across 2 findings

Disable the rlogin service and use alternatives like SSH instead.

> Affected service: 513/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugins 1.3.6.1.4.1.25623.1.0.113766, 1.3.6.1.4.1.25623.1.0.901202 after the change; they should stop reporting on the affected asset. |

## A14 Follow the scanner's stated remediation on 1 asset — covers 2 instances across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "The repaired package can be downloaded from the referenced vendor homepage. Please validate the package with its signature." That instruction identifies its target only by context, and this finding was observed on more than one service, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Covers 2 distinct services (21/tcp, 6200/tcp). The scanner states one remediation for all of them; confirm it applies to each before treating this as a single change.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.103185; it should stop reporting. |

## A15 Certificate / cryptographic configuration on 1 asset — covers 2 instances across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore. Please see the references for more resources supporting you with this task." That instruction identifies its target only by context, and this finding was observed on more than one service, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Covers 2 distinct services (25/tcp, 5432/tcp). The scanner states one remediation for all of them; confirm it applies to each before treating this as a single change.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A15. |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.103440; it should stop reporting. |

## A16 Certificate / cryptographic configuration on 1 asset — covers 2 instances across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "- Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group. Please see the references for more resources supporting you with this task. - For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits." That instruction identifies its target only by context, and this finding was observed on more than one service, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Covers 2 distinct services (25/tcp, 5432/tcp). The scanner states one remediation for all of them; confirm it applies to each before treating this as a single change.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.106223; it should stop reporting. |

## A17 Follow the scanner's stated remediation on 1 asset — covers 2 instances across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Change the password as soon as possible." That instruction identifies its target only by context, and this finding was observed on more than one service, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Covers 2 distinct services (21/tcp, 2121/tcp). The scanner states one remediation for all of them; confirm it applies to each before treating this as a single change.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.108718; it should stop reporting. |

## A18 Certificate / cryptographic configuration on 1 asset — covers 2 instances across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1.2+ protocols. Please see the references for more resources supporting you with this task." That instruction identifies its target only by context, and this finding was observed on more than one service, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Covers 2 distinct services (25/tcp, 5432/tcp). The scanner states one remediation for all of them; confirm it applies to each before treating this as a single change.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A18. |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.111012; it should stop reporting. |

## A19 Certificate / cryptographic configuration on 1 asset — covers 2 instances across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more resources supporting you with this task." That instruction identifies its target only by context, and this finding was observed on more than one service, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Covers 2 distinct services (25/tcp, 5432/tcp). The scanner states one remediation for all of them; confirm it applies to each before treating this as a single change.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A19. |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.117274; it should stop reporting. |

## A20 Certificate / cryptographic configuration on 1 asset — resolves 2 instances across 1 finding

- DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should be considered. - Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For Postfix this limit can be configured via 'smtpd_client_new_tls_session_rate_limit' option, for other products please refer to the manual of the product in question on configuration possibilities.

> Covers 2 distinct services (25/tcp, 5432/tcp). The scanner states one remediation for all of them; confirm it applies to each before treating this as a single change.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A20. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.117840 after the change; it should stop reporting on the affected asset. |

## A21 Certificate / cryptographic configuration on 1 asset — resolves 2 instances across 1 finding

Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.

> Covers 2 distinct services (21/tcp, 2121/tcp). The scanner states one remediation for all of them; confirm it applies to each before treating this as a single change.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.108528 after the change; it should stop reporting on the affected asset. |

## A22 Certificate / cryptographic configuration on 1 asset — resolves 2 instances across 1 finding

Replace the certificate with a stronger key and reissue the certificates it signed.

> Covers 2 distinct services (25/tcp, 5432/tcp). The scanner states one remediation for all of them; confirm it applies to each before treating this as a single change.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.150710 after the change; it should stop reporting on the affected asset. |

## A23 Certificate / cryptographic configuration on 1 asset — resolves 2 instances across 1 finding

Replace the SSL/TLS certificate by a new one.

> Covers 2 distinct services (25/tcp, 5432/tcp). The scanner states one remediation for all of them; confirm it applies to each before treating this as a single change.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.103955 after the change; it should stop reporting on the affected asset. |

## A24 Certificate / cryptographic configuration on 1 asset — resolves 2 instances across 1 finding

Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

> Covers 2 distinct services (25/tcp, 5432/tcp). The scanner states one remediation for all of them; confirm it applies to each before treating this as a single change.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.105880 after the change; it should stop reporting on the affected asset. |

## A25 Certificate / cryptographic configuration on 1 asset — resolves 2 instances across 1 finding

Users should contact their vendors for specific patch information. A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.

> Covers 2 distinct services (25/tcp, 5432/tcp). The scanner states one remediation for all of them; confirm it applies to each before treating this as a single change.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A25. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.117761 after the change; it should stop reporting on the affected asset. |

## A26 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 2.11.9.5 / 3.1.3.1 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.100077 after the change; it should stop reporting on the affected asset. |

## A27 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 3.1.3.1 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.100078 after the change; it should stop reporting on the affected asset. |

## A28 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 2.2.9 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 2.2.9 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A28. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.100211 after the change; it should stop reporting on the affected asset. |

## A29 Follow the scanner's stated remediation on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Updates are available. Please see the references for more information." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 5432/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A29. |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.100273; it should stop reporting. |

## A30 Follow the scanner's stated remediation on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Updates are available. Please see the references for more information." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 445/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A30. |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.100306; it should stop reporting. |

## A31 Vendor patch / advisory on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Vendor updates are available. Please see the references for details." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A31. |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.100307; it should stop reporting. |

## A32 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 1.3.2b, 1.3.3rc2 or later.

| | |
|---|---|
| Version target | Fixed version (stated by the scanner): 1.3.2b |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A32. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.100316 after the change; it should stop reporting on the affected asset. |

## A33 Follow the scanner's stated remediation on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Updates are available. Please see the references for more information." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A33. |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.100359; it should stop reporting. |

## A34 Follow the scanner's stated remediation on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Updates are available. Please see the references for more information." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 5432/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A34. |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.100400; it should stop reporting. |

## A35 Follow the scanner's stated remediation on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Updates are available. Please see the references for more information." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 5432/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A35. |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.100470; it should stop reporting. |

## A36 Follow the scanner's stated remediation on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Updates are available. Please see the references for more information." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 445/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A36. |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.100476; it should stop reporting. |

## A37 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.2.14, 5.3.3 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A37. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.100529 after the change; it should stop reporting on the affected asset. |

## A38 Follow the scanner's stated remediation on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Updates are available. Please see the references for more information." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A38. |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.100582; it should stop reporting. |

## A39 Follow the scanner's stated remediation on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Updates are available. Please see the references for more information." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A39. |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.100583; it should stop reporting. |

## A40 Follow the scanner's stated remediation on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Updates are available. Please see the references for more information." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 445/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A40. |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.100623; it should stop reporting. |

## A41 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.2.14, 5.3.2 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.100631 after the change; it should stop reporting on the affected asset. |

## A42 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 3.4.8, 3.5.2 or later.

> Affected service: 445/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A42. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.100644 after the change; it should stop reporting on the affected asset. |

## A43 Follow the scanner's stated remediation on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Updates are available. Please see the references for more information." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 5432/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A43. |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.100645; it should stop reporting. |

## A44 Follow the scanner's stated remediation on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Updates are available. Please see the references for more information." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 5432/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A44. |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.100648; it should stop reporting. |

## A45 Follow the scanner's stated remediation on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Updates are available. Please see the references for more information." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 445/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A45. |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.100680; it should stop reporting. |

## A46 Follow the scanner's stated remediation on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Updates are available. Please see the references for details." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A46. |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.100684; it should stop reporting. |

## A47 Follow the scanner's stated remediation on 1 asset — resolves 1 instance across 1 finding

These issues have been fixed in Apache 2.2.16. Please see the references for more information.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A47. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.100725 after the change; it should stop reporting on the affected asset. |

## A48 Follow the scanner's stated remediation on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Updates are available. Please see the references for more information." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A48. |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.100726; it should stop reporting. |

## A49 Follow the scanner's stated remediation on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Updates are available. Please see the references for details." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A49. |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.100761; it should stop reporting. |

## A50 Vendor patch / advisory on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Vendor updates are available. Please see the references for more information." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.100775; it should stop reporting. |

## A51 Follow the scanner's stated remediation on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Updates are available. Please see the references for more information." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 445/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A51. |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.100803; it should stop reporting. |

## A52 Follow the scanner's stated remediation on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Updates are available. Please see the references for more information." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 5432/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A52. |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.100843; it should stop reporting. |

## A53 Follow the scanner's stated remediation on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Updates are available. Please see the references for more information." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A53. |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.100898; it should stop reporting. |

## A54 Vendor patch / advisory on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Vendor updates are available. Please see the references for more information." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A54. |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.100939; it should stop reporting. |

## A55 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.2.17, 5.3.5 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A55. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.103020 after the change; it should stop reporting on the affected asset. |

## A56 Follow the scanner's stated remediation on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Updates are available. Please see the references for more information." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 5432/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A56. |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.103054; it should stop reporting. |

## A57 Follow the scanner's stated remediation on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Updates are available. Please see the references for details." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A57. |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.103076; it should stop reporting. |

## A58 Follow the scanner's stated remediation on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Updates are available. Please see the references for more information." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 445/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A58. |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.103095; it should stop reporting. |

## A59 Follow the scanner's stated remediation on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Updates are available. Please see the references for more information." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 445/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.103283; it should stop reporting. |

## A60 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 1.3.3g or later.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 1.3.3g |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A60. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.103331 after the change; it should stop reporting on the affected asset. |

## A61 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 2.3.5 or later.

> Affected service: 21/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 2.3.5 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.103362 after the change; it should stop reporting on the affected asset. |

## A62 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.3.11, 5.4.1 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A62. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.103486 after the change; it should stop reporting on the affected asset. |

## A63 Follow the scanner's stated remediation on 1 asset — resolves 1 instance across 1 finding

Change the password as soon as possible.

> Affected service: 5432/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.103552 after the change; it should stop reporting on the affected asset. |

## A64 Vendor patch / advisory on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Vendor updates are available. Please see the references for more information. For more information about DistCC's security see the references." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 3632/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A64. |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.103553; it should stop reporting. |

## A65 Follow the scanner's stated remediation on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Updates are available. Please see the references for more information." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 25/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A65. |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.103935; it should stop reporting. |

## A66 Follow the scanner's stated remediation on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Updates are available. Please see the references for details." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 22/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A66. |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.103937; it should stop reporting. |

## A67 Follow the scanner's stated remediation on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Updates are available. Please see the references for more information." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 22/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A67. |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.103939; it should stop reporting. |

## A68 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 4.14.14, 4.15.9, 4.16.4 or later.

> Affected service: 445/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A68. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.104259 after the change; it should stop reporting on the affected asset. |

## A69 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 7.4.31, 8.0.24, 8.1.11 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A69. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.104331 after the change; it should stop reporting on the affected asset. |

## A70 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 4.15.12, 4.16.7, 4.17.3 or later.

> Affected service: 445/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A70. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.104423 after the change; it should stop reporting on the affected asset. |

## A71 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 4.15.13, 4.16.0 or later.

> Affected service: 445/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A71. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.104475 after the change; it should stop reporting on the affected asset. |

## A72 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 4.15.13, 4.16.8, 4.17.4 or later.

> Affected service: 445/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A72. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.104476 after the change; it should stop reporting on the affected asset. |

## A73 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 9.2 or later.

> Affected service: 22/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 9.2 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.104512 after the change; it should stop reporting on the affected asset. |

## A74 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 8.0.28, 8.1.16, 8.2.3 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A74. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.104541 after the change; it should stop reporting on the affected asset. |

## A75 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 9.3 or later.

> Affected service: 22/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 9.3 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.104635 after the change; it should stop reporting on the affected asset. |

## A76 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 8.0.22, 8.1.9, 8.2.0 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A76. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.104644 after the change; it should stop reporting on the affected asset. |

## A77 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 4.16.11, 4.17.10, 4.18.5 or later.

> Affected service: 445/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A77. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.104872 after the change; it should stop reporting on the affected asset. |

## A78 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 4.17.12, 4.18.8, 4.19.1 or later.

> Affected service: 445/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A78. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.104957 after the change; it should stop reporting on the affected asset. |

## A79 Follow the scanner's stated remediation on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Updates are available. Please see the references for more information." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 22/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A79. |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.105001; it should stop reporting. |

## A80 Follow the scanner's stated remediation on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Updates are available. Please see the references for more information." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 22/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A80. |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.105003; it should stop reporting. |

## A81 Follow the scanner's stated remediation on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Updates are available. Please see the references for more information." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 22/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A81. |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.105004; it should stop reporting. |

## A82 Follow the scanner's stated remediation on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Updates are available. Please see the references for more information." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 5432/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A82. |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.105042; it should stop reporting. |

## A83 Follow the scanner's stated remediation on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Updates are available. Please see the references or vendor advisory for more information." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 445/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A83. |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.105231; it should stop reporting. |

## A84 Configuration change on 1 asset — resolves 1 instance across 1 finding

Change the password to something hard to guess or enable password protection at all.

> Affected service: 5900/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.106056 after the change; it should stop reporting on the affected asset. |

## A85 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 1.3.6b, 1.3.7rc2 or later.

| | |
|---|---|
| Version target | Fixed version (stated by the scanner): 1.3.6b |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A85. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.107734 after the change; it should stop reporting on the affected asset. |

## A86 Follow the scanner's stated remediation on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Updates are available. Please see the referenced vendor advisory." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 445/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.108011; it should stop reporting. |

## A87 Follow the scanner's stated remediation on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Updates are available. Please see the referenced vendor advisory." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 445/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.108012; it should stop reporting. |

## A88 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 3.0.3 or later.

> Affected service: 21/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 3.0.3 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A88. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.108045 after the change; it should stop reporting on the affected asset. |

## A89 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.6.30, 7.0.15, 7.1.1 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A89. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.108052 after the change; it should stop reporting on the affected asset. |

## A90 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 3.3.10.3, 3.4.3.2 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A90. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.108242 after the change; it should stop reporting on the affected asset. |

## A91 Vendor patch / advisory on 1 asset — resolves 1 instance across 1 finding

Update to Apache HTTP Server 2.4.28. For Apache HTTP Server running version 2.2.34 apply the patch linked in the references. As a workaround the usage of .htaccess should be disabled completely via the 'AllowOverride None' directive within the webservers configuration. Furthermore all <Limit> statements within the webserver configuration needs to be verified for invalid HTTP methods.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A91. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.108252 after the change; it should stop reporting on the affected asset. |

## A92 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.6.39, 7.0.33, 7.1.26, 7.2.14, 7.3.0 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A92. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.108505 after the change; it should stop reporting on the affected asset. |

## A93 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 7.1.32, 7.3.9 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A93. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.108633 after the change; it should stop reporting on the affected asset. |

## A94 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 7.1.32 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 7.1.32 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.108635 after the change; it should stop reporting on the affected asset. |

## A95 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 7.2.22, 7.3.9 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.108637 after the change; it should stop reporting on the affected asset. |

## A96 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 7.1.33, 7.2.24, 7.3.11 or later. As an alternative a workaround to update the nginx configuration to mitigate this vulnerability is described at the PHP.net bugtracker linked in the references.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A96. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.108692 after the change; it should stop reporting on the affected asset. |

## A97 Configuration change on 1 asset — resolves 1 instance across 1 finding

Disable the TRACE and TRACK methods in your web server configuration. Please see the manual of your web server or the references for more information.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A97. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.11213 after the change; it should stop reporting on the affected asset. |

## A98 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 10.6 or 11.1 respectively.

> Affected service: 5432/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A98. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.112429 after the change; it should stop reporting on the affected asset. |

## A99 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 4.9.5, 5.0.2 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A99. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.112715 after the change; it should stop reporting on the affected asset. |

## A100 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 4.8.3.

> Affected service: 80/tcp.

| | |
|---|---|
| Version target | Fixed version (stated by the scanner): 4.8.3 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A100. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.113255 after the change; it should stop reporting on the affected asset. |

## A101 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 1.3.7 or later.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 1.3.7 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A101. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.113645 after the change; it should stop reporting on the affected asset. |

## A102 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 9.5.25, 9.6.21, 10.16, 11.11, 12.6 or 13.2 respectively.

> Affected service: 5432/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A102. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.113791 after the change; it should stop reporting on the affected asset. |

## A103 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 8.1.30, 8.2.24, 8.3.12 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A103. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.114787 after the change; it should stop reporting on the affected asset. |

## A104 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 7.3.29 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 7.3.29 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A104. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.117524 after the change; it should stop reporting on the affected asset. |

## A105 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 7.3.31, 7.4.24, 8.0.11 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A105. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.117694 after the change; it should stop reporting on the affected asset. |

## A106 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 4.13.13, 4.14.9, 4.15.1 or later.

> Affected service: 445/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A106. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.117760 after the change; it should stop reporting on the affected asset. |

## A107 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 4.9.15, 4.10.10, 4.11.2 or later.

> Affected service: 445/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A107. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.117772 after the change; it should stop reporting on the affected asset. |

## A108 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 8.0 or later.

> Affected service: 22/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 8.0 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A108. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.117786 after the change; it should stop reporting on the affected asset. |

## A109 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.4.4 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 5.4.4 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.117788 after the change; it should stop reporting on the affected asset. |

## A110 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 7.0.12 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 7.0.12 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A110. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.117800 after the change; it should stop reporting on the affected asset. |

## A111 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.6.29, 7.0.14 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A111. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.117803 after the change; it should stop reporting on the affected asset. |

## A112 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 9.6 or later. Note: Client and Server implementations need to run a fixed version to mitigate the Terrapin flaw.

> Affected service: 22/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 9.6 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A112. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.118572 after the change; it should stop reporting on the affected asset. |

## A113 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 4.17.1 or later.

> Affected service: 445/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 4.17.1 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A113. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.126184 after the change; it should stop reporting on the affected asset. |

## A114 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 9.1 or later.

> Affected service: 22/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 9.1 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.127244 after the change; it should stop reporting on the affected asset. |

## A115 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 4.8.6 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 4.8.6 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A115. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.140207 after the change; it should stop reporting on the affected asset. |

## A116 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 3.0.0 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 3.0.0 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A116. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.141635 after the change; it should stop reporting on the affected asset. |

## A117 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 1.6.3 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 1.6.3 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A117. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.141637 after the change; it should stop reporting on the affected asset. |

## A118 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 6.1.0 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 6.1.0 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.141830 after the change; it should stop reporting on the affected asset. |

## A119 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.6.40, 7.1.16, 7.2.14, 7.3.1 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A119. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.142048 after the change; it should stop reporting on the affected asset. |

## A120 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 3.4.0 or later. Patch diffs are available for older versions.

> Affected service: 80/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 3.4.0 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A120. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.142314 after the change; it should stop reporting on the affected asset. |

## A121 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 1.3.6 or later.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 1.3.6 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A121. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.143205 after the change; it should stop reporting on the affected asset. |

## A122 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 1.3.6c or later.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 1.3.6c |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A122. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.143206 after the change; it should stop reporting on the affected asset. |

## A123 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 4.9.4, 5.0.1 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A123. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.143346 after the change; it should stop reporting on the affected asset. |

## A124 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 7.2.27, 7.3.14, 7.4.2 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A124. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.143392 after the change; it should stop reporting on the affected asset. |

## A125 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 9.4.26, 9.5.21, 9.6.17, 10.12, 11.7, 12.2 or later.

> Affected service: 5432/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A125. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.143610 after the change; it should stop reporting on the affected asset. |

## A126 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 7.2.30, 7.3.17, 7.4.5 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A126. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.143722 after the change; it should stop reporting on the affected asset. |

## A127 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 7.2.31, 7.3.18, 7.4.6 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A127. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.143913 after the change; it should stop reporting on the affected asset. |

## A128 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 7.2.34, 7.3.23, 7.4.11 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A128. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.144694 after the change; it should stop reporting on the affected asset. |

## A129 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 9.5.23, 9.6.19, 10.14, 11.9, 12.4 or later.

> Affected service: 5432/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A129. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.144709 after the change; it should stop reporting on the affected asset. |

## A130 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 4.9.6, 5.0.3 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A130. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.144896 after the change; it should stop reporting on the affected asset. |

## A131 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 7.3.26, 7.4.14, 8.0.1 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A131. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.145114 after the change; it should stop reporting on the affected asset. |

## A132 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 7.3.27, 7.4.15, 8.0.2 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A132. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.145323 after the change; it should stop reporting on the affected asset. |

## A133 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 7.3.28, 7.4.18 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.145869 after the change; it should stop reporting on the affected asset. |

## A134 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 7.3.30, 7.4.23, 8.0.10 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.146584 after the change; it should stop reporting on the affected asset. |

## A135 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 4.14.8 or later.

> Affected service: 445/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 4.14.8 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A135. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.146864 after the change; it should stop reporting on the affected asset. |

## A136 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 2.2.32, 2.4.25 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A136. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.147044 after the change; it should stop reporting on the affected asset. |

## A137 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 2.2.27, 2.4.9 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A137. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.147047 after the change; it should stop reporting on the affected asset. |

## A138 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 2.2.29, 2.4.12 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A138. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.147048 after the change; it should stop reporting on the affected asset. |

## A139 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 2.2.25, 2.4.6 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A139. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.147050 after the change; it should stop reporting on the affected asset. |

## A140 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 2.2.25 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 2.2.25 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A140. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.147051 after the change; it should stop reporting on the affected asset. |

## A141 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 2.2.24, 2.4.4 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A141. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.147052 after the change; it should stop reporting on the affected asset. |

## A142 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 2.2.23, 2.4.3 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A142. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.147055 after the change; it should stop reporting on the affected asset. |

## A143 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 2.2.23, 2.4.2 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A143. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.147056 after the change; it should stop reporting on the affected asset. |

## A144 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 2.0.65, 2.2.19 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A144. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.147060 after the change; it should stop reporting on the affected asset. |

## A145 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 4.13.14, 4.14.10, 4.15.2 or later.

> Affected service: 445/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A145. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.147124 after the change; it should stop reporting on the affected asset. |

## A146 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 9.6.24, 10.19, 11.14, 12.9, 13.5, 14.1 or later.

> Affected service: 5432/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A146. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.147148 after the change; it should stop reporting on the affected asset. |

## A147 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 7.3.33, 7.4.26, 8.0.13 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A147. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.147187 after the change; it should stop reporting on the affected asset. |

## A148 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 4.15.0 or later.

> Affected service: 445/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 4.15.0 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A148. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.147401 after the change; it should stop reporting on the affected asset. |

## A149 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 4.13.17, 4.14.12, 4.15.5 or later.

> Affected service: 445/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A149. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.147554 after the change; it should stop reporting on the affected asset. |

## A150 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 4.15.5 or later.

> Affected service: 445/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 4.15.5 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A150. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.147555 after the change; it should stop reporting on the affected asset. |

## A151 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 7.4.28, 8.0.16, 8.1.3 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A151. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.147657 after the change; it should stop reporting on the affected asset. |

## A152 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 4.9.10, 5.1.3 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A152. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.147786 after the change; it should stop reporting on the affected asset. |

## A153 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 7.4.30, 8.0.20, 8.1.7 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A153. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.148249 after the change; it should stop reporting on the affected asset. |

## A154 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 7.4.33, 8.0.25, 8.1.12 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A154. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.148830 after the change; it should stop reporting on the affected asset. |

## A155 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 8.0.27, 8.1.14, 8.2.1 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A155. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.149069 after the change; it should stop reporting on the affected asset. |

## A156 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 8.0.29, 8.1.10, 8.2.7 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A156. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.149760 after the change; it should stop reporting on the affected asset. |

## A157 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.7 or later.

> Affected service: 22/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 5.7 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.150632 after the change; it should stop reporting on the affected asset. |

## A158 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 4.9 or later.

> Affected service: 22/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 4.9 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.150633 after the change; it should stop reporting on the affected asset. |

## A159 Vendor patch / advisory on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Apply the patch mentioned in the linked reference." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 445/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.150722; it should stop reporting. |

## A160 Vendor patch / advisory on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Apply the patch mentioned in the linked reference." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 445/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.150725; it should stop reporting. |

## A161 Vendor patch / advisory on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Apply the patch mentioned in the linked reference." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 445/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A161. |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.150728; it should stop reporting. |

## A162 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 3.4.16, 3.5.14, 3.6.4 or later.

> Affected service: 445/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A162. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.150729 after the change; it should stop reporting on the affected asset. |

## A163 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 3.5.22, 3.6.17, 4.0.8 or later.

> Affected service: 445/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A163. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.150732 after the change; it should stop reporting on the affected asset. |

## A164 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 4.1.22, 4.2.7, 4.3.3 or later.

> Affected service: 445/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A164. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.150746 after the change; it should stop reporting on the affected asset. |

## A165 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 8.1.28, 8.2.18, 8.3.6 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A165. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.152118 after the change; it should stop reporting on the affected asset. |

## A166 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 8.1.29, 8.2.20, 8.3.8 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A166. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.152369 after the change; it should stop reporting on the affected asset. |

## A167 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 8.1.31, 8.2.26, 8.3.14 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A167. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.153495 after the change; it should stop reporting on the affected asset. |

## A168 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 13.19, 14.16, 15.11, 16.7, 17.3 or later.

> Affected service: 5432/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A168. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.154018 after the change; it should stop reporting on the affected asset. |

## A169 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 8.1.32, 8.2.28 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A169. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.154187 after the change; it should stop reporting on the affected asset. |

## A170 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 13.21, 14.18, 15.13, 16.9, 17.5 or later.

> Affected service: 5432/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A170. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.154470 after the change; it should stop reporting on the affected asset. |

## A171 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 8.1.33, 8.2.29, 8.3.23, 8.4.10 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A171. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.154869 after the change; it should stop reporting on the affected asset. |

## A172 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 13.22, 14.19, 15.14, 16.10, 17.6 or later.

> Affected service: 5432/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A172. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.155168 after the change; it should stop reporting on the affected asset. |

## A173 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 1.3.8b or later.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 1.3.8b |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A173. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.155383 after the change; it should stop reporting on the affected asset. |

## A174 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 1.3.8c or later.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 1.3.8c |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A174. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.155384 after the change; it should stop reporting on the affected asset. |

## A175 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 1.3.9 or later.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 1.3.9 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A175. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.155385 after the change; it should stop reporting on the affected asset. |

## A176 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 13.23, 14.20, 15.15, 16.11, 17.7, 18.1 or later.

> Affected service: 5432/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A176. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.155797 after the change; it should stop reporting on the affected asset. |

## A177 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 8.2.30, 8.3.29, 8.4.16 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A177. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.156071 after the change; it should stop reporting on the affected asset. |

## A178 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 8.0.30, 8.1.22, 8.2.9 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A178. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.170529 after the change; it should stop reporting on the affected asset. |

## A179 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 4.2.4 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 4.2.4 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.800320 after the change; it should stop reporting on the affected asset. |

## A180 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Upgrade to version 2.11.9.5 or 3.1.3.1 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.800381 after the change; it should stop reporting on the affected asset. |

## A181 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.2.9 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 5.2.9 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A181. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.800393 after the change; it should stop reporting on the affected asset. |

## A182 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Upgrade to version 4.3.1 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 4.3.1 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.800400 after the change; it should stop reporting on the affected asset. |

## A183 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 2.3.3 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 2.3.3 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A183. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.800827 after the change; it should stop reporting on the affected asset. |

## A184 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 2.2.12 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 2.2.12 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A184. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.800837 after the change; it should stop reporting on the affected asset. |

## A185 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.2.11, 5.3.1 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A185. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.801060 after the change; it should stop reporting on the affected asset. |

## A186 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.2.12, 5.3.1 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A186. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.801123 after the change; it should stop reporting on the affected asset. |

## A187 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.2.14, 5.3.3 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A187. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.801359 after the change; it should stop reporting on the affected asset. |

## A188 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.2.15, 5.3.4 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A188. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.801547 after the change; it should stop reporting on the affected asset. |

## A189 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.2.15, 5.3.4 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A189. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.801586 after the change; it should stop reporting on the affected asset. |

## A190 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 1.3.3c or later.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 1.3.3c |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A190. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.801639 after the change; it should stop reporting on the affected asset. |

## A191 Follow the scanner's stated remediation on 1 asset — resolves 1 instance across 1 finding

- Update to PHP version 5.5.2 or later and set 'session.use_strict_mode' in php.ini to 'On'
- make adoptive session with user land code as described in the referenced PHP strict_sessions document

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A191. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.803737 after the change; it should stop reporting on the affected asset. |

## A192 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.3.22, 5.4.12 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A192. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.803764 after the change; it should stop reporting on the affected asset. |

## A193 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.3.29, 5.4.24, 5.5.8 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A193. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.804160 after the change; it should stop reporting on the affected asset. |

## A194 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.3.28, 5.4.23, 5.5.7 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A194. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.804174 after the change; it should stop reporting on the affected asset. |

## A195 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.4.32, 5.5.16 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A195. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.804292 after the change; it should stop reporting on the affected asset. |

## A196 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.4.29, 5.5.13 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A196. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.804639 after the change; it should stop reporting on the affected asset. |

## A197 Version upgrade on 1 asset — resolves 1 instance across 1 finding

- Remove support for 'RSA_EXPORT' cipher suites from the service. Please see the references for more resources supporting you with this task. - If the service is using OpenSSL: Update to version 0.9.8zd, 1.0.0p, 1.0.1k or later.

> Affected service: 25/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A197. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.805142 after the change; it should stop reporting on the affected asset. |

## A198 Follow the scanner's stated remediation on 1 asset — resolves 1 instance across 1 finding

Update to PHP version 5.5.21, 5.6.5 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A198. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.805412 after the change; it should stop reporting on the affected asset. |

## A199 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.4.37 or 5.5.21 or 5.6.5 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A199. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.805414 after the change; it should stop reporting on the affected asset. |

## A200 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 2.4.13 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 2.4.13 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A200. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.805616 after the change; it should stop reporting on the affected asset. |

## A201 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.4.39, 5.5.23, 5.6.7 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A201. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.805651 after the change; it should stop reporting on the affected asset. |

## A202 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.4.40, 5.5.24, 5.6.8 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A202. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.805657 after the change; it should stop reporting on the affected asset. |

## A203 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.4.40, 5.5.24, 5.6.8 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A203. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.805658 after the change; it should stop reporting on the affected asset. |

## A204 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.4.41, 5.5.25, 5.6.9 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A204. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.805660 after the change; it should stop reporting on the affected asset. |

## A205 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.4.38, 5.5.22, 5.6.6 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A205. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.805685 after the change; it should stop reporting on the affected asset. |

## A206 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.5.24, 5.6.8 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A206. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.805687 after the change; it should stop reporting on the affected asset. |

## A207 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 9.0.20, 9.1.16, 9.2.11, 9.3.7, 9.4.2 or later.

> Affected service: 5432/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A207. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.805805 after the change; it should stop reporting on the affected asset. |

## A208 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.5.30, 5.6.14 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A208. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.806649 after the change; it should stop reporting on the affected asset. |

## A209 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.4.44, 5.5.28, 5.6.12 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A209. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.807503 after the change; it should stop reporting on the affected asset. |

## A210 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.5.31, 5.6.17, 7.0.2 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A210. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.807504 after the change; it should stop reporting on the affected asset. |

## A211 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.4.45, 5.5.29, 5.6.13 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A211. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.807505 after the change; it should stop reporting on the affected asset. |

## A212 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.4.43, 5.5.27, 5.6.11 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A212. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.807507 after the change; it should stop reporting on the affected asset. |

## A213 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Upgrade to version 9.1.20 or 9.2.15 or 9.3.11 or 9.4.6 or 9.5.1 or later.

> Affected service: 5432/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A213. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.807518 after the change; it should stop reporting on the affected asset. |

## A214 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Upgrade to samba version 4.2.11, or 4.3.8, or 4.4.2, or later.

> Affected service: 445/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A214. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.807646 after the change; it should stop reporting on the affected asset. |

## A215 Follow the scanner's stated remediation on 1 asset — resolves 1 instance across 1 finding

Update to PHP version 5.5.33, 5.6.19 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A215. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.807807 after the change; it should stop reporting on the affected asset. |

## A216 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.5.34, 5.6.20, 7.0.5 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A216. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.808199 after the change; it should stop reporting on the affected asset. |

## A217 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.5.35, 5.6.21, 7.0.6 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A217. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.808603 after the change; it should stop reporting on the affected asset. |

## A218 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.4.44, 5.5.28, 5.6.12 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A218. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.808604 after the change; it should stop reporting on the affected asset. |

## A219 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.5.32, 5.6.18, 7.0.3 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A219. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.808607 after the change; it should stop reporting on the affected asset. |

## A220 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.6.18, 7.0.3 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A220. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.808609 after the change; it should stop reporting on the affected asset. |

## A221 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.5.28, 5.6.12 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.808613 after the change; it should stop reporting on the affected asset. |

## A222 Follow the scanner's stated remediation on 1 asset — resolves 1 instance across 1 finding

Update to PHP version 5.5.22, 5.6.6 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A222. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.808615 after the change; it should stop reporting on the affected asset. |

## A223 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.4.45, 5.5.29, 5.6.13 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A223. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.808617 after the change; it should stop reporting on the affected asset. |

## A224 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.6.24, 7.0.9 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A224. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.808628 after the change; it should stop reporting on the affected asset. |

## A225 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 2.4.24, or 2.2.32, or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A225. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.808632 after the change; it should stop reporting on the affected asset. |

## A226 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.5.38, 5.6.24, 7.0.9 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A226. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.808634 after the change; it should stop reporting on the affected asset. |

## A227 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Upgrade to version 9.1.23 or 9.2.18 or 9.3.14 or 9.4.9 or 9.5.4 or higher.

> Affected service: 5432/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A227. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.808665 after the change; it should stop reporting on the affected asset. |

## A228 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.4.44, 5.5.28, 5.6.12, 7.0.4 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A228. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.808666 after the change; it should stop reporting on the affected asset. |

## A229 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.5.27, 5.6.11 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A229. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.808671 after the change; it should stop reporting on the affected asset. |

## A230 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.4.42, 5.5.26, 5.6.10 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A230. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.808675 after the change; it should stop reporting on the affected asset. |

## A231 Follow the scanner's stated remediation on 1 asset — resolves 1 instance across 1 finding

Update to PHP version 5.5.37, 5.6.23, 7.0.8 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A231. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.808788 after the change; it should stop reporting on the affected asset. |

## A232 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.5.37, 5.6.23 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A232. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.808790 after the change; it should stop reporting on the affected asset. |

## A233 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.5.36, 5.6.22 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A233. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.808792 after the change; it should stop reporting on the affected asset. |

## A234 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.5.36, 5.6.22, 7.0.7 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A234. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.808794 after the change; it should stop reporting on the affected asset. |

## A235 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.4.38, 5.5.22, 5.6.6 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A235. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.809137 after the change; it should stop reporting on the affected asset. |

## A236 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.5.31, 5.6.17, 7.0.2 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A236. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.809139 after the change; it should stop reporting on the affected asset. |

## A237 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 7.3 or later.

> Affected service: 22/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 7.3 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A237. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.809154 after the change; it should stop reporting on the affected asset. |

## A238 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.6.26, 7.0.11 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A238. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.809317 after the change; it should stop reporting on the affected asset. |

## A239 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.6.25, 7.0.10 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A239. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.809319 after the change; it should stop reporting on the affected asset. |

## A240 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.6.27, 7.0.12 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A240. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.809338 after the change; it should stop reporting on the affected asset. |

## A241 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 7.4 or later.

> Affected service: 22/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 7.4 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A241. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.8103256 after the change; it should stop reporting on the affected asset. |

## A242 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 1.3.5e, 1.3.6rc5 or later.

| | |
|---|---|
| Version target | Fixed version (stated by the scanner): 1.3.5e |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A242. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.810731 after the change; it should stop reporting on the affected asset. |

## A243 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 7.2 or later.

> Affected service: 22/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 7.2 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A243. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.810769 after the change; it should stop reporting on the affected asset. |

## A244 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.6.31, 7.0.21, 7.1.7 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A244. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.811482 after the change; it should stop reporting on the affected asset. |

## A245 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.6.31, 7.0.17, 7.1.3 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A245. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.811487 after the change; it should stop reporting on the affected asset. |

## A246 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.6.28, 7.0.13 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A246. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.811489 after the change; it should stop reporting on the affected asset. |

## A247 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Upgrade to Samba 4.6.8, 4.5.14 and 4.4.16 or later.

> Affected service: 445/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A247. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.811905 after the change; it should stop reporting on the affected asset. |

## A248 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 7.6 or later.

> Affected service: 22/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 7.6 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A248. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.812051 after the change; it should stop reporting on the affected asset. |

## A249 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.6.32, 7.0.25, 7.1.11 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A249. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.812073 after the change; it should stop reporting on the affected asset. |

## A250 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.5.32, 5.6.18, 7.0.3 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A250. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.812512 after the change; it should stop reporting on the affected asset. |

## A251 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 7.1.20, 7.2.8, 7.3.0alpha3 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A251. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.812520 after the change; it should stop reporting on the affected asset. |

## A252 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.6.33, 7.0.27, 7.1.13, 7.2.1 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A252. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.812735 after the change; it should stop reporting on the affected asset. |

## A253 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.6.34, 7.0.28, 7.1.15, 7.2.3 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A253. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.812821 after the change; it should stop reporting on the affected asset. |

## A254 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.6.36, 7.0.30, 7.1.17, 7.2.5 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A254. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.813160 after the change; it should stop reporting on the affected asset. |

## A255 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.6.35, 7.0.29, 7.1.16, 7.2.4 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A255. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.813162 after the change; it should stop reporting on the affected asset. |

## A256 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Upgrade to version 4.8.2 or newer. Please see the references for more information.

> Affected service: 80/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 4.8.2 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A256. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.813451 after the change; it should stop reporting on the affected asset. |

## A257 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 7.8 or later.

> Affected service: 22/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 7.8 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A257. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.813864 after the change; it should stop reporting on the affected asset. |

## A258 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 5.6.37, 7.0.31, 7.1.20 or 7.2.8 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A258. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.813901 after the change; it should stop reporting on the affected asset. |

## A259 Follow the scanner's stated remediation on 1 asset — resolves 1 instance across 1 finding

Fixed is available in the SVN repository, please see the references for more information.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A259. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.900107 after the change; it should stop reporting on the affected asset. |

## A260 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Upgrade to respective version below, PostgreSQL 8.3.7 or 8.2.13 or 8.1.17 or 8.0.21 or 7.4.25.

> Affected service: 5432/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A260. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.900480 after the change; it should stop reporting on the affected asset. |

## A261 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 3.3.6 or later.

> Affected service: 445/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): 3.3.6 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A261. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.900685 after the change; it should stop reporting on the affected asset. |

## A262 Follow the scanner's stated remediation on 1 asset — resolves 1 instance across 1 finding

Update to Apache HTTP Server version 2.0.64, 2.2.14 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A262. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.900842 after the change; it should stop reporting on the affected asset. |

## A263 Certificate / cryptographic configuration on 1 asset — resolves 1 instance across 1 finding

- DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should be considered. - Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For OpenSSH this limit can be configured via the 'MaxStartups' option, for other products please refer to the manual of the product in question on configuration possibilities.

> Affected service: 22/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A263. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.117839 after the change; it should stop reporting on the affected asset. |

## A264 Follow the scanner's stated remediation on 1 asset — resolves 1 instance across 1 finding

- Update Apache Tomcat to version 7.0.100, 8.5.51, 9.0.31 or later - For other products using Tomcat please contact the vendor for more information on fixed versions

> Affected service: 8009/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A264. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.143545 after the change; it should stop reporting on the affected asset. |

## A265 Follow the scanner's stated remediation on 1 asset — resolves 1 instance across 1 finding

A whole cleanup of the infected system is recommended.

> Affected service: 1524/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.103549 after the change; it should stop reporting on the affected asset. |

## A266 Configuration change on 1 asset — resolves 1 instance across 1 finding

Administrators of environments that rely on Distributed Ruby should ensure that appropriate controls are in place. Code-level controls may include: - Implementing taint on untrusted input - Setting $SAFE levels appropriately (>=2 is recommended if untrusted hosts are allowed to submit Ruby commands, and >=3 may be appropriate) - Including drb/acl.rb to set ACLEntry to restrict access to trusted hosts

> Affected service: 8787/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.108010 after the change; it should stop reporting on the affected asset. |

## A267 Version upgrade on 1 asset — resolves 1 instance across 1 finding

All Samba users should upgrade to the latest version.

> Affected service: 445/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.90028 after the change; it should stop reporting on the affected asset. |

## A268 Configuration change on 1 asset — resolves 1 instance across 1 finding

As a workaround disable mod_copy in the ProFTPD configuration file.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A268. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.142662 after the change; it should stop reporting on the affected asset. |

## A269 Configuration change on 1 asset — resolves 1 instance across 1 finding

Delete the listed files or restrict access to them.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.11229 after the change; it should stop reporting on the affected asset. |

## A270 Configuration change on 1 asset — resolves 1 instance across 1 finding

Disable class-loading. Please contact the vendor of the affected system for additional guidance.

> Affected service: 1099/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A270. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.140051 after the change; it should stop reporting on the affected asset. |

## A271 Configuration change on 1 asset — resolves 1 instance across 1 finding

**Remove the weak algorithms from the SSH server's offer**

The scanner names the offending algorithms in its own report for the host, then says to disable them without saying where. For an OpenSSH server the answer is sshd_config: Ciphers, MACs, KexAlgorithms and HostKeyAlgorithms, one keyword per family the scan reported. Prefer the subtractive form. OpenSSH reads a list beginning with '-' as "remove these from my defaults" and accepts wildcards there, while a plain list REPLACES the defaults outright and freezes the algorithm set at whatever was typed on the day — which is how a hardening change becomes next year's outage, when clients have moved on and the server no longer offers anything they support. Do not assume OpenSSH: these checks fire against anything answering SSH, and a Dropbear build, a network appliance or an embedded stack is configured somewhere else entirely, so confirm the implementation before editing a file that may not be the one in use. Keep a second session open while applying it — a syntax error in sshd_config stops the daemon from starting.

```
# /etc/ssh/sshd_config - subtractive, so OpenSSH's own defaults keep improving
Ciphers -*-cbc
MACs -*-sha1,*-sha1-96,*-md5
KexAlgorithms -*sha1,diffie-hellman-group-exchange-sha1
HostKeyAlgorithms -ssh-rsa,ssh-dss
```

> Affected service: 22/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Alternative mitigation | Where a legacy client genuinely cannot negotiate anything stronger, reduce exposure while it is replaced rather than leaving the algorithms offered to the whole network: reach the service only from a management network or a jump host. The finding stays open until the algorithms are actually removed from the server's offer. |
| Operational impact | The affected service must be reloaded or restarted before the change takes effect. sshd rereads its configuration on SIGHUP by re-executing itself, so the change applies to connections made afterwards. OpenSSH's documentation does not state what happens to sessions already established, so schedule as though a brief interruption is possible rather than assuming there is none. Removing a host key algorithm is the one to stage carefully: a client that has the server's old key pinned in known_hosts and cannot negotiate the remaining algorithm will refuse the connection rather than warn. |
| Guidance source | Reviewed playbook — remediation confirmed for this check by review, not taken from the scanner's text. (playbook greenbone-ssh-weak-algorithms v1, reviewed 2026-09-06) |
| Validation | Read the effective configuration back from the daemon rather than the file, so an override elsewhere in sshd_config cannot hide the change, then confirm from a client that the server no longer offers the reported algorithms. Re-run the scan last: it is the check that the scanner agrees, not the check that the change worked. |

> sshd -T | grep -Ei '^(ciphers|macs|kexalgorithms|hostkeyalgorithms) '

Playbook references

OpenBSD, sshd_config(5) - the '+' and '-' list modifiers for Ciphers, MACs and KexAlgorithms

> https://man.openbsd.org/sshd_config

OpenBSD, sshd(8) - SIGHUP causes sshd to reread its configuration by re-executing itself

> https://man.openbsd.org/sshd

## A272 Configuration change on 1 asset — resolves 1 instance across 1 finding

**Remove the weak algorithms from the SSH server's offer**

The scanner names the offending algorithms in its own report for the host, then says to disable them without saying where. For an OpenSSH server the answer is sshd_config: Ciphers, MACs, KexAlgorithms and HostKeyAlgorithms, one keyword per family the scan reported. Prefer the subtractive form. OpenSSH reads a list beginning with '-' as "remove these from my defaults" and accepts wildcards there, while a plain list REPLACES the defaults outright and freezes the algorithm set at whatever was typed on the day — which is how a hardening change becomes next year's outage, when clients have moved on and the server no longer offers anything they support. Do not assume OpenSSH: these checks fire against anything answering SSH, and a Dropbear build, a network appliance or an embedded stack is configured somewhere else entirely, so confirm the implementation before editing a file that may not be the one in use. Keep a second session open while applying it — a syntax error in sshd_config stops the daemon from starting.

```
# /etc/ssh/sshd_config - subtractive, so OpenSSH's own defaults keep improving
Ciphers -*-cbc
MACs -*-sha1,*-sha1-96,*-md5
KexAlgorithms -*sha1,diffie-hellman-group-exchange-sha1
HostKeyAlgorithms -ssh-rsa,ssh-dss
```

> Affected service: 22/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Alternative mitigation | Where a legacy client genuinely cannot negotiate anything stronger, reduce exposure while it is replaced rather than leaving the algorithms offered to the whole network: reach the service only from a management network or a jump host. The finding stays open until the algorithms are actually removed from the server's offer. |
| Operational impact | The affected service must be reloaded or restarted before the change takes effect. sshd rereads its configuration on SIGHUP by re-executing itself, so the change applies to connections made afterwards. OpenSSH's documentation does not state what happens to sessions already established, so schedule as though a brief interruption is possible rather than assuming there is none. Removing a host key algorithm is the one to stage carefully: a client that has the server's old key pinned in known_hosts and cannot negotiate the remaining algorithm will refuse the connection rather than warn. |
| Guidance source | Reviewed playbook — remediation confirmed for this check by review, not taken from the scanner's text. (playbook greenbone-ssh-weak-algorithms v1, reviewed 2026-09-06) |
| Validation | Read the effective configuration back from the daemon rather than the file, so an override elsewhere in sshd_config cannot hide the change, then confirm from a client that the server no longer offers the reported algorithms. Re-run the scan last: it is the check that the scanner agrees, not the check that the change worked. |

```
sshd -T | grep -Ei '^(ciphers|macs|kexalgorithms|hostkeyalgorithms) '
```

Playbook references

OpenBSD, sshd_config(5) - the '+' and '-' list modifiers for Ciphers, MACs and KexAlgorithms

> https://man.openbsd.org/sshd_config

OpenBSD, sshd(8) - SIGHUP causes sshd to reread its configuration by re-executing itself

> https://man.openbsd.org/sshd

## A273 Configuration change on 1 asset — resolves 1 instance across 1 finding

**Remove the weak algorithms from the SSH server's offer**

The scanner names the offending algorithms in its own report for the host, then says to disable them without saying where. For an OpenSSH server the answer is sshd_config: Ciphers, MACs, KexAlgorithms and HostKeyAlgorithms, one keyword per family the scan reported. Prefer the subtractive form. OpenSSH reads a list beginning with '-' as "remove these from my defaults" and accepts wildcards there, while a plain list REPLACES the defaults outright and freezes the algorithm set at whatever was typed on the day — which is how a hardening change becomes next year's outage, when clients have moved on and the server no longer offers anything they support. Do not assume OpenSSH: these checks fire against anything answering SSH, and a Dropbear build, a network appliance or an embedded stack is configured somewhere else entirely, so confirm the implementation before editing a file that may not be the one in use. Keep a second session open while applying it — a syntax error in sshd_config stops the daemon from starting.

```
# /etc/ssh/sshd_config - subtractive, so OpenSSH's own defaults keep improving
Ciphers -*-cbc
MACs -*-sha1,*-sha1-96,*-md5
KexAlgorithms -*sha1,diffie-hellman-group-exchange-sha1
HostKeyAlgorithms -ssh-rsa,ssh-dss
```

> Affected service: 22/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Alternative mitigation | Where a legacy client genuinely cannot negotiate anything stronger, reduce exposure while it is replaced rather than leaving the algorithms offered to the whole network: reach the service only from a management network or a jump host. The finding stays open until the algorithms are actually removed from the server's offer. |
| Operational impact | The affected service must be reloaded or restarted before the change takes effect. sshd rereads its configuration on SIGHUP by re-executing itself, so the change applies to connections made afterwards. OpenSSH's documentation does not state what happens to sessions already established, so schedule as though a brief interruption is possible rather than assuming there is none. Removing a host key algorithm is the one to stage carefully: a client that has the server's old key pinned in known_hosts and cannot negotiate the remaining algorithm will refuse the connection rather than warn. |
| Guidance source | Reviewed playbook — remediation confirmed for this check by review, not taken from the scanner's text. (playbook greenbone-ssh-weak-algorithms v1, reviewed 2026-09-06) |
| Validation | Read the effective configuration back from the daemon rather than the file, so an override elsewhere in sshd_config cannot hide the change, then confirm from a client that the server no longer offers the reported algorithms. Re-run the scan last: it is the check that the scanner agrees, not the check that the change worked. |

```
sshd -T | grep -Ei '^(ciphers|macs|kexalgorithms|hostkeyalgorithms) '
```

Playbook references

OpenBSD, sshd_config(5) - the '+' and '-' list modifiers for Ciphers, MACs and KexAlgorithms

> https://man.openbsd.org/sshd_config

OpenBSD, sshd(8) - SIGHUP causes sshd to reread its configuration by re-executing itself

> https://man.openbsd.org/sshd

## A274 Configuration change on 1 asset — resolves 1 instance across 1 finding

Disable the rexec service and use alternatives like SSH instead.

> Affected service: 512/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.100111 after the change; it should stop reporting on the affected asset. |

## A275 Configuration change on 1 asset — resolves 1 instance across 1 finding

Disable the rsh service and use alternatives like SSH instead.

> Affected service: 514/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.100080 after the change; it should stop reporting on the affected asset. |

## A276 Configuration change on 1 asset — resolves 1 instance across 1 finding

Disable VRFY and/or EXPN on your Mailserver. For postfix add 'disable_vrfy_command=yes' in 'main.cf'. For Sendmail add the option 'O PrivacyOptions=goaway'. It is suggested that, if you really want to publish this type of information, you use a mechanism that legitimate users actually know about, such as Finger or HTTP.

> Affected service: 25/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.100072 after the change; it should stop reporting on the affected asset. |

## A277 Certificate / cryptographic configuration on 1 asset — resolves 1 instance across 1 finding

Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.108440 after the change; it should stop reporting on the affected asset. |

## A278 Configuration change on 1 asset — resolves 1 instance across 1 finding

If not needed disable the directory listing/indexing within the web servers config.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.111074 after the change; it should stop reporting on the affected asset. |

## A279 Configuration change on 1 asset — resolves 1 instance across 1 finding

If you do not want to share files, you should disable anonymous logins.

> Affected service: 21/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.900600 after the change; it should stop reporting on the affected asset. |

## A280 Version upgrade on 1 asset — resolves 1 instance across 1 finding

PHP: Update to version 5.3.13, 5.4.3 or later - Other products / applications: Please contact the vendor for a solution

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A280. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.103482 after the change; it should stop reporting on the affected asset. |

## A281 Follow the scanner's stated remediation on 1 asset — resolves 1 instance across 1 finding

Replace Telnet with a protocol like SSH which supports encrypted connections.

> Affected service: 23/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.108522 after the change; it should stop reporting on the affected asset. |

## A282 Follow the scanner's stated remediation on 1 asset — resolves 1 instance across 1 finding

Run the session over an encrypted channel provided by IPsec [RFC4301] or SSH [RFC4254]. Some VNC server vendors are also providing more secure Security Types within their products.

> Affected service: 5900/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.108529 after the change; it should stop reporting on the affected asset. |

## A283 Follow the scanner's stated remediation on 1 asset — resolves 1 instance across 1 finding

Update jQuery on the remote host to a still supported version.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.117149 after the change; it should stop reporting on the affected asset. |

## A284 Follow the scanner's stated remediation on 1 asset — resolves 1 instance across 1 finding

Update the Apache HTTP Server version on the remote host to a still supported version.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.108085 after the change; it should stop reporting on the affected asset. |

## A285 Follow the scanner's stated remediation on 1 asset — resolves 1 instance across 1 finding

Update the OS on the remote host to a version which is still supported and receiving security updates by the vendor. Note / Important: Please create an override for this result if the target host is a: - Windows system with Extended Security Updates (ESU) - System with additional 3rd-party / non-vendor security updates like e.g. from 'TuxCare', 'Freexian Extended LTS' or similar

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.103674 after the change; it should stop reporting on the affected asset. |

## A286 Follow the scanner's stated remediation on 1 asset — resolves 1 instance across 1 finding

Update the PHP version on the remote host to a still supported version.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.105889 after the change; it should stop reporting on the affected asset. |

## A287 Follow the scanner's stated remediation on 1 asset — resolves 1 instance across 1 finding

Update the phpMyAdmin version on the remote host to a still supported version.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.113015 after the change; it should stop reporting on the affected asset. |

## A288 Follow the scanner's stated remediation on 1 asset — resolves 1 instance across 1 finding

Update the PostgreSQL version on the remote host to a still supported version.

> Affected service: 5432/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.140158 after the change; it should stop reporting on the affected asset. |

## A289 Follow the scanner's stated remediation on 1 asset — resolves 1 instance across 1 finding

Update the Samba version on the remote host to a still supported version.

> Affected service: 445/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.140159 after the change; it should stop reporting on the affected asset. |

## A290 Follow the scanner's stated remediation on 1 asset — resolves 1 instance across 1 finding

Update to Apache HTTP Server 2.2.32 or 2.4.25 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A290. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.812033 after the change; it should stop reporting on the affected asset. |

## A291 Follow the scanner's stated remediation on 1 asset — resolves 1 instance across 1 finding

Update to Apache HTTP Server 2.2.33 or 2.4.26 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A291. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.811214 after the change; it should stop reporting on the affected asset. |

## A292 Follow the scanner's stated remediation on 1 asset — resolves 1 instance across 1 finding

Update to Apache HTTP Server 2.2.34 or 2.4.27 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A292. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.811237 after the change; it should stop reporting on the affected asset. |

## A293 Follow the scanner's stated remediation on 1 asset — resolves 1 instance across 1 finding

Update to PHP 5.2.15 or 5.3.4

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A293. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.801583 after the change; it should stop reporting on the affected asset. |

## A294 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 7.1p2 or later.

> Affected service: 22/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A294. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.806671 after the change; it should stop reporting on the affected asset. |

## A295 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 7.2p2 or later.

> Affected service: 22/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A295. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.105581 after the change; it should stop reporting on the affected asset. |

## A296 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 7.2p2-3 or later.

> Affected service: 22/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A296. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.807574 after the change; it should stop reporting on the affected asset. |

## A297 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to version 9.3p2 or later.

> Affected service: 22/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A297. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.104869 after the change; it should stop reporting on the affected asset. |

## A298 Version upgrade on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Updates are available. Update to newer Version." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 5432/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A298. |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.100157; it should stop reporting. |

## A299 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Upgrade to phpMyAdmin version 3.2.0.1 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A299. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.800595 after the change; it should stop reporting on the affected asset. |

## A300 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Upgrade to PostgreSQL version 9.2.21 or 9.3.17 or 9.4.12 or 9.5.7 or 9.6.3 or later.

> Affected service: 5432/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A300. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.810990 after the change; it should stop reporting on the affected asset. |

## A301 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Upgrade to Samba 4.4.10 or 4.5.6 or later.

> Affected service: 445/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A301. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.811083 after the change; it should stop reporting on the affected asset. |

## A302 Configuration change on 1 asset — resolves 1 instance across 1 finding

Use access restrictions for the /doc directory. If you use Apache you might use this in your access.conf: <Directory /usr/doc> AllowOverride None order deny, allow deny from all allow from localhost </Directory>

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.10056 after the change; it should stop reporting on the affected asset. |

## A303 Configuration change on 1 asset — resolves 1 instance across 1 finding

Use access restrictions to these dangerous HTTP methods or disable them completely.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.10498 after the change; it should stop reporting on the affected asset. |

## A304 Vendor patch / advisory on 1 asset — covers 1 instance across 1 finding

Authoritative product-specific remediation for this finding could not be confirmed.

> The scanner stated: "Vendor updates are available." The report contains no product-specific fix or retrievable advisory behind that reference, so it is reproduced here as the scanner's words rather than stated as the recommended action.

> Affected service: 80/tcp.

| | |
|---|---|
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Manual review required — authoritative product-specific remediation could not be confirmed. |
| Validation | No confirmed fix to validate. Once a remediation is chosen and applied, rescan with plugin 1.3.6.1.4.1.25623.1.0.100144; it should stop reporting. |

## A305 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Update to Apache HTTP Server version 2.2.22 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): Apache HTTP Server 2.2.22 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A305. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.902830 after the change; it should stop reporting on the affected asset. |

## A306 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Upgrade to OpenSSH version 6.9 or later.

> Affected service: 22/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): OpenSSH 6.9 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A306. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.806049 after the change; it should stop reporting on the affected asset. |

## A307 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Upgrade to OpenSSH 7.0 or later.

> Affected service: 22/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): OpenSSH 7.0 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A307. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.806052 after the change; it should stop reporting on the affected asset. |

## A308 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Upgrade to phpMyAdmin version 3.3.7 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): phpMyAdmin 3.3.7 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Vendor reference detail | See scanner evidence appendix for A308. |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.801286 after the change; it should stop reporting on the affected asset. |

### A309 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Upgrade to TWiki version 4.3.2 or later.

> Affected service: 80/tcp.

| | |
|---|---|
| Version target | Minimum fixed version stated by the scanner (an open range — a later version may be required): TWiki 4.3.2 |
| Highest EPSS (covered findings) | no CVE among covered findings |
| Guidance source | Scanner-supplied — the wording above is the scanner's own solution text. |
| Validation | Rescan with plugin 1.3.6.1.4.1.25623.1.0.801281 after the change; it should stop reporting on the affected asset. |

## Lower-priority and informational items

Unless a line says otherwise, its remediation category and any plugin pointer come from the scanner's own solution text.

**A1** No scanner-supplied solution — manual review: covers 100 instances across 79 findings on 1 asset. Affected services: 1099/tcp, 111/tcp, 139/tcp, 1524/tcp, 21/tcp, 2121/tcp; 15 additional affected services not shown here.

**A310** Certificate / cryptographic configuration: covers 2 instances across 1 finding on 1 asset; see plugin 1.3.6.1.4.1.25623.1.0.802087 in the scan. Affected services: 25/tcp, 5432/tcp.

**A311** Scanner-stated remediation, not categorized — product-specific remediation not confirmed: covers 1 instance across 1 finding on 1 asset; see plugin 1.3.6.1.4.1.25623.1.0.100158 in the scan. Affected services: 5432/tcp.

**A312** Configuration change: covers 1 instance across 1 finding on 1 asset; see plugin 1.3.6.1.4.1.25623.1.0.100488 in the scan. Affected services: 445/tcp.

**A313** Version upgrade: covers 1 instance across 1 finding on 1 asset; see plugin 1.3.6.1.4.1.25623.1.0.100499 in the scan. Affected services: 445/tcp.

**A314** Scanner-stated remediation, not categorized — product-specific remediation not confirmed: covers 1 instance across 1 finding on 1 asset; see plugin 1.3.6.1.4.1.25623.1.0.103298 in the scan. Affected services: 445/tcp.

**A315** Configuration change: covers 1 instance across 1 finding on 1 asset; see plugin 1.3.6.1.4.1.25623.1.0.10342 in the scan. Affected services: 5900/tcp.

**A316** Scanner-stated remediation, not categorized — product-specific remediation not confirmed: covers 1 instance across 1 finding on 1 asset; see plugin 1.3.6.1.4.1.25623.1.0.103503 in the scan. Affected services: 22/tcp.

**A317** Scanner-stated remediation, not categorized — product-specific remediation not confirmed: covers 1 instance across 1 finding on 1 asset; see plugin 1.3.6.1.4.1.25623.1.0.105002 in the scan. Affected services: 22/tcp.

**A318** Version upgrade: covers 1 instance across 1 finding on 1 asset; see plugin 1.3.6.1.4.1.25623.1.0.117876 in the scan. Affected services: 445/tcp.

**A319** Version upgrade: covers 1 instance across 1 finding on 1 asset; see plugin 1.3.6.1.4.1.25623.1.0.119134 in the scan. Affected services: 22/tcp.

**A320** Configuration change: covers 1 instance across 1 finding on 1 asset; see plugin 1.3.6.1.4.1.25623.1.0.119214 in the scan. Affected services: 22/tcp.

**A321** Version upgrade: covers 1 instance across 1 finding on 1 asset; see plugin 1.3.6.1.4.1.25623.1.0.144365 in the scan. Affected services: 80/tcp.

**A322** Version upgrade: covers 1 instance across 1 finding on 1 asset; see plugin 1.3.6.1.4.1.25623.1.0.150648 in the scan. Affected services: 22/tcp.

**A323** Version upgrade: covers 1 instance across 1 finding on 1 asset; see plugin 1.3.6.1.4.1.25623.1.0.800373 in the scan. Affected services: 80/tcp.

**A324** Configuration change: covers 1 instance across 1 finding on 1 asset; see plugin 1.3.6.1.4.1.25623.1.0.80091 in the scan.

**A325** Version upgrade: covers 1 instance across 1 finding on 1 asset; see plugin 1.3.6.1.4.1.25623.1.0.805188 in the scan. Affected services: 25/tcp.

**A326** Scanner-stated remediation, not categorized: covers 1 instance across 1 finding on 1 asset; see plugin 1.3.6.1.4.1.25623.1.0.900841 in the scan. Affected services: 80/tcp.

**A327** Vendor patch / advisory: covers 1 instance across 1 finding on 1 asset; see plugin 1.3.6.1.4.1.25623.1.0.902139 in the scan. Affected services: 5432/tcp.

**A328** Configuration change: covers 1 instance across 1 finding on 1 asset; see plugin 1.3.6.1.4.1.25623.1.0.105610 in the scan. Affected services: 22/tcp.

**A329** Scanner-stated remediation, not categorized: covers 1 instance across 1 finding on 1 asset; see plugin 1.3.6.1.4.1.25623.1.0.103333 in the scan. Affected services: 80/tcp.

**A330** Configuration change: covers 1 instance across 1 finding on 1 asset; see plugin 1.3.6.1.4.1.25623.1.0.103190 in the scan.

**A331** Version upgrade: covers 1 instance across 1 finding on 1 asset; see plugin 1.3.6.1.4.1.25623.1.0.117252 in the scan. Affected services: 80/tcp.

**A332** Version upgrade: covers 1 instance across 1 finding on 1 asset; see plugin 1.3.6.1.4.1.25623.1.0.100153 in the scan. Affected services: 22/tcp.

## Top urgent findings

> EPSS estimates the likelihood of exploitation in roughly the next 30 days. It complements CISA KEV and CVSS and replaces neither: KEV records past exploitation, CVSS states technical severity, and EPSS estimates near-term exploitation probability.

a deterministic synthetic EPSS feed generated by tools/synthetic_epss_feed.py (not real EPSS data), retrieved 2026-09-13, model score date 2026-08-30.

| # | Priority / band | Issue | Hosts | Instances |
|---|---|---|---|---|
| 1 | Band 5<br>no CVE, non-trivial severity<br>**Schedule** | **The rexec service is running** Plugin 1.3.6.1.4.1.25623.1.0.100111 —<br>KEV: No CVE to check against CISA KEV — EPSS: no scored CVE for this issue — CVSS: 10.0 (v2.0) — Exploit available: Unknown<br>Technical risk (Greenbone summary) This remote host is running a rexec service. See appendix | 1 | 1 |
| 2 | Band 5<br>no CVE, non-trivial severity<br>**Schedule** | **PHP < 5.2.12 Multiple Vulnerabilities** Plugin 1.3.6.1.4.1.25623.1.0.100409 —<br>KEV: No CVE to check against CISA KEV — EPSS: no scored CVE for this issue — CVSS: 10.0 (v2.0) — Exploit available: Unknown<br>Technical risk (Greenbone summary) PHP is prone to multiple vulnerabilities. See appendix | 1 | 1 |
| 3 | Band 5<br>no CVE, non-trivial severity<br>**Schedule** | **Apache HTTP Server Multiple Security Vulnerabilities** Plugin 1.3.6.1.4.1.25623.1.0.100514 —<br>KEV: No CVE to check against CISA KEV — EPSS: no scored CVE for this issue — CVSS: 10.0 (v2.0) — Exploit available: Unknown<br>Technical risk (Greenbone summary) Apache HTTP Server is prone to multiple vulnerabilities. See appendix | 1 | 1 |
| 4 | Band 5<br>no CVE, non-trivial severity<br>**Schedule** | **PHP 5.3.x < 5.3.7 Multiple Security Vulnerabilities** Plugin 1.3.6.1.4.1.25623.1.0.103229 —<br>KEV: No CVE to check against CISA KEV — EPSS: no scored CVE for this issue — CVSS: 10.0 (v2.0) — Exploit available: Unknown<br>Technical risk (Greenbone summary) PHP is prone to multiple vulnerabilities. See appendix | 1 | 1 |
| 5 | Band 5<br>no CVE, non-trivial severity<br>**Schedule** | **Possible Backdoor: Ingreslock** Plugin 1.3.6.1.4.1.25623.1.0.103549 —<br>KEV: No CVE to check against CISA KEV — EPSS: no scored CVE for this issue — CVSS: 10.0 (v2.0) — Exploit available: Unknown<br>Technical risk (Greenbone summary) A backdoor is installed on the remote host. See appendix | 1 | 1 |
| 6 | Band 5<br>no CVE, non-trivial severity<br>**Schedule** | **Operating System (OS) End of Life (EOL) Detection** Plugin 1.3.6.1.4.1.25623.1.0.103674 —<br>KEV: No CVE to check against CISA KEV — EPSS: no scored CVE for this issue — CVSS: 10.0 (v2.0) — Exploit available: Unknown<br>Technical risk (Greenbone summary) The Operating System (OS) on the remote host has reached the end of life (EOL) and should not be used anymore. See appendix | 1 | 1 |
| 7 | Band 5<br>no CVE, non-trivial severity<br>**Schedule** | **Samba 'TALLOC_FREE()' Function RCE Vulnerability** Plugin 1.3.6.1.4.1.25623.1.0.105231 —<br>KEV: No CVE to check against CISA KEV — EPSS: no scored CVE for this issue — CVSS: 10.0 (v2.0) — Exploit available: Unknown<br>Technical risk (Greenbone summary) Samba is prone to a remote code execution (RCE) vulnerability in the 'TALLOC_FREE()' function. See appendix | 1 | 1 |

| # | Priority / band | Issue | Hosts | Instances |
|---|---|---|---|---|
| 8 | Band 5<br>no CVE, non-trivial severity<br>**Schedule** | **PHP End of Life (EOL) Detection - Linux** Plugin 1.3.6.1.4.1.25623.1.0.105889 —<br>KEV: No CVE to check against CISA KEV — EPSS: no scored CVE for this issue — CVSS: 10.0 (v2.0) — Exploit available: Unknown<br>Technical risk (Greenbone summary) The PHP version on the remote host has reached the end of life (EOL) and should not be used anymore. See appendix | 1 | 1 |
| 9 | Band 5<br>no CVE, non-trivial severity<br>**Schedule** | **Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities** Plugin 1.3.6.1.4.1.25623.1.0.108010 —<br>KEV: No CVE to check against CISA KEV — EPSS: no scored CVE for this issue — CVSS: 10.0 (v2.0) — Exploit available: Unknown<br>Technical risk (Greenbone summary) Systems using Distributed Ruby (dRuby/DRb), which is available in Ruby versions 1.6 and later, may permit unauthorized systems to execute distributed commands. See appendix | 1 | 1 |
| 10 | Band 5<br>no CVE, non-trivial severity<br>**Schedule** | **Apache HTTP Server End of Life (EOL) Detection - Linux** Plugin 1.3.6.1.4.1.25623.1.0.108085 —<br>KEV: No CVE to check against CISA KEV — EPSS: no scored CVE for this issue — CVSS: 10.0 (v2.0) — Exploit available: Unknown<br>Technical risk (Greenbone summary) The Apache HTTP Server version on the remote host has reached the End of Life (EOL) and should not be used anymore. See appendix | 1 | 1 |
| 11 | Band 5<br>no CVE, non-trivial severity<br>**Schedule** | **PHP < 5.2.7 Multiple Vulnerabilities** Plugin 1.3.6.1.4.1.25623.1.0.108868 —<br>KEV: No CVE to check against CISA KEV — EPSS: no scored CVE for this issue — CVSS: 10.0 (v2.0) — Exploit available: Unknown<br>Technical risk (Greenbone summary) PHP is prone to multiple vulnerabilities. See appendix | 1 | 1 |
| 12 | Band 5<br>no CVE, non-trivial severity<br>**Schedule** | **phpMyAdmin End of Life (EOL) Detection - Linux** Plugin 1.3.6.1.4.1.25623.1.0.113015 —<br>KEV: No CVE to check against CISA KEV — EPSS: no scored CVE for this issue — CVSS: 10.0 (v2.0) — Exploit available: Unknown<br>Technical risk (Greenbone summary) The phpMyAdmin version on the remote host has reached the End of Life (EOL) and should not be used anymore. See appendix | 1 | 1 |
| 13 | Band 5<br>no CVE, non-trivial severity<br>**Schedule** | **rlogin Passwordless Login** Plugin 1.3.6.1.4.1.25623.1.0.113766 —<br>KEV: No CVE to check against CISA KEV — EPSS: no scored CVE for this issue — CVSS: 10.0 (v2.0) — Exploit available: Unknown<br>Technical risk (Greenbone summary) The rlogin service allows root access without a password. See appendix | 1 | 1 |

| # | Priority / band | Issue | Hosts | Instances |
|---|---|---|---|---|
| 14 | Band 5<br>no CVE, non-trivial severity<br>**Schedule** | **PostgreSQL End of Life (EOL) Detection - Linux** Plugin 1.3.6.1.4.1.25623.1.0.140158 —<br>KEV: No CVE to check against CISA KEV — EPSS: no scored CVE for this issue — CVSS: 10.0 (v2.0) — Exploit available: Unknown<br>Technical risk (Greenbone summary) The PostgreSQL version on the remote host has reached the End of Life (EOL) and should not be used anymore. See appendix | 1 | 1 |
| 15 | Band 5<br>no CVE, non-trivial severity<br>**Schedule** | **Samba End of Life (EOL) Detection** Plugin 1.3.6.1.4.1.25623.1.0.140159 —<br>KEV: No CVE to check against CISA KEV — EPSS: no scored CVE for this issue — CVSS: 10.0 (v2.0) — Exploit available: Unknown<br>Technical risk (Greenbone summary) The Samba version on the remote host has reached the end of life (EOL) and should not be used anymore. See appendix | 1 | 1 |
| 16 | Band 5<br>no CVE, non-trivial severity<br>**Schedule** | **Samba 3.0.0 <= 3.0.25rc3 Remote Code Execution Vulnerability (CVE-2007-2446)** Plugin 1.3.6.1.4.1.25623.1.0.150725 —<br>KEV: No CVE to check against CISA KEV — EPSS: no scored CVE for this issue — CVSS: 10.0 (v2.0) — Exploit available: Unknown<br>Technical risk (Greenbone summary) Multiple Heap Overflows Allow remote code execution (RCE). See appendix | 1 | 1 |
| 17 | Band 5<br>no CVE, non-trivial severity<br>**Schedule** | **Samba 3.0.0 <= 3.6.3 Remote Code Execution Vulnerability (CVE-2012-1182)** Plugin 1.3.6.1.4.1.25623.1.0.150729 —<br>KEV: No CVE to check against CISA KEV — EPSS: no scored CVE for this issue — CVSS: 10.0 (v2.0) — Exploit available: Unknown<br>Technical risk (Greenbone summary) Samba 3.0.x to 3.6.3 are affected by a vulnerability that allows remote code execution (RCE) as the 'root' user. See appendix | 1 | 1 |
| 18 | Band 5<br>no CVE, non-trivial severity<br>**Schedule** | **PostgreSQL Multiple Vulnerabilities (Aug 2025) - Linux** Plugin 1.3.6.1.4.1.25623.1.0.155168 —<br>KEV: No CVE to check against CISA KEV — EPSS: no scored CVE for this issue — CVSS: 10.0 (v2.0) — Exploit available: Unknown<br>Technical risk (Greenbone summary) PostgreSQL is prone to multiple vulnerabilities. See appendix | 1 | 1 |
| 19 | Band 5<br>no CVE, non-trivial severity<br>**Schedule** | **TWiki < 4.2.4 Multiple XSS / Command Execution Vulnerabilities** Plugin 1.3.6.1.4.1.25623.1.0.800320 —<br>KEV: No CVE to check against CISA KEV — EPSS: no scored CVE for this issue — CVSS: 10.0 (v2.0) — Exploit available: Unknown<br>Technical risk (Greenbone summary) TWiki is prone to multiple cross-site scripting (XSS) and command execution vulnerabilities. See appendix | 1 | 1 |
| 20 | Band 5<br>no CVE, non-trivial severity<br>**Schedule** | **ProFTPD < 1.3.3c Multiple Vulnerabilities** Plugin 1.3.6.1.4.1.25623.1.0.801639 —<br>KEV: No CVE to check against CISA KEV — EPSS: no scored CVE for this issue — CVSS: 10.0 (v2.0) — Exploit available: Unknown<br>Technical risk (Greenbone summary) ProFTPD is prone to multiple vulnerabilities. See appendix | 1 | 1 |

349 further findings in the technical appendix.

# Technical appendix

## #1 The rexec service is running

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100111

| | |
|---|---|
| CVEs | — |
| CVSS base score | 10.0 |
| Remediation | Addressed by remediation action A274 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 512/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 10.0. Severity rating 4 (derived from CVSS). |
| Rank position | Position 1 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:C/I:C/A:C — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #2 PHP < 5.2.12 Multiple Vulnerabilities

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100409

| | |
|---|---|
| CVEs | — |
| CVSS base score | 10.0 |
| Remediation | Addressed by remediation action A2 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 10.0. Severity rating 4 (derived from CVSS). |
| Rank position | Position 2 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:C/I:C/A:C — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #3 Apache HTTP Server Multiple Security Vulnerabilities

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100514

| | |
|---|---|
| CVEs | — |
| CVSS base score | 10.0 |
| Remediation | Addressed by remediation action A9 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 10.0. Severity rating 4 (derived from CVSS). |
| Rank position | Position 3 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:C/I:C/A:C — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #4 PHP 5.3.x < 5.3.7 Multiple Security Vulnerabilities

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.103229

| | |
|---|---|
| CVEs | — |
| CVSS base score | 10.0 |
| Remediation | Addressed by remediation action A4 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 10.0. Severity rating 4 (derived from CVSS). |
| Rank position | Position 4 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:C/I:C/A:C — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #5 Possible Backdoor: Ingreslock

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.103549

| | |
|---|---|
| CVEs | — |
| CVSS base score | 10.0 |
| Remediation | Addressed by remediation action A265 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 1524/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 10.0. Severity rating 4 (derived from CVSS). |
| Rank position | Position 5 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:C/I:C/A:C — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #6 Operating System (OS) End of Life (EOL) Detection

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.103674

| | |
|---|---|
| CVEs | — |
| CVSS base score | 10.0 |
| Remediation | Addressed by remediation action A285 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default general |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 10.0. Severity rating 4 (derived from CVSS). |
| Rank position | Position 6 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:C/I:C/A:C — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #7 Samba 'TALLOC_FREE()' Function RCE Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.105231

| | |
|---|---|
| CVEs | — |
| CVSS base score | 10.0 |
| Remediation | Addressed by remediation action A83 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 445/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 10.0. Severity rating 4 (derived from CVSS). |
| Rank position | Position 7 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:C/I:C/A:C — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #8 PHP End of Life (EOL) Detection - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.105889

| | |
|---|---|
| CVEs | — |
| CVSS base score | 10.0 |
| Remediation | Addressed by remediation action A286 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 10.0. Severity rating 4 (derived from CVSS). |
| Rank position | Position 8 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:C/I:C/A:C — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #9 Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.108010

| | |
|---|---|
| CVEs | — |
| CVSS base score | 10.0 |
| Remediation | Addressed by remediation action A266 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 8787/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 10.0. Severity rating 4 (derived from CVSS). |
| Rank position | Position 9 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:C/I:C/A:C — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #10 Apache HTTP Server End of Life (EOL) Detection - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.108085

| | |
|---|---|
| CVEs | — |
| CVSS base score | 10.0 |
| Remediation | Addressed by remediation action A284 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 10.0. Severity rating 4 (derived from CVSS). |
| Rank position | Position 10 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:C/I:C/A:C — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #11 PHP < 5.2.7 Multiple Vulnerabilities

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.108868

| | |
|---|---|
| CVEs | — |
| CVSS base score | 10.0 |
| Remediation | Addressed by remediation action A2 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 10.0. Severity rating 4 (derived from CVSS). |
| Rank position | Position 11 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:C/I:C/A:C — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #12 phpMyAdmin End of Life (EOL) Detection - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.113015

| | |
|---|---|
| CVEs | — |
| CVSS base score | 10.0 |
| Remediation | Addressed by remediation action A287 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 10.0. Severity rating 4 (derived from CVSS). |
| Rank position | Position 12 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:C/I:C/A:C — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #13 rlogin Passwordless Login

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.113766

| | |
|---|---|
| CVEs | — |
| CVSS base score | 10.0 |
| Remediation | Addressed by remediation action A13 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 513/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 10.0. Severity rating 4 (derived from CVSS). |
| Rank position | Position 13 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:C/I:C/A:C — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #14 PostgreSQL End of Life (EOL) Detection - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.140158

| | |
|---|---|
| CVEs | — |
| CVSS base score | 10.0 |
| Remediation | Addressed by remediation action A288 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 5432/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 10.0. Severity rating 4 (derived from CVSS). |
| Rank position | Position 14 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:C/I:C/A:C — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #15 Samba End of Life (EOL) Detection

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.140159

| | |
|---|---|
| CVEs | — |
| CVSS base score | 10.0 |
| Remediation | Addressed by remediation action A289 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 445/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 10.0. Severity rating 4 (derived from CVSS). |
| Rank position | Position 15 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:C/I:C/A:C — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #16 Samba 3.0.0 <= 3.0.25rc3 Remote Code Execution Vulnerability (CVE-2007-2446)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.150725

| | |
|---|---|
| CVEs | — |
| CVSS base score | 10.0 |
| Remediation | Addressed by remediation action A160 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 445/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 10.0. Severity rating 4 (derived from CVSS). |
| Rank position | Position 16 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:C/I:C/A:C — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #17 Samba 3.0.0 <= 3.6.3 Remote Code Execution Vulnerability (CVE-2012-1182)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.150729

| | |
|---|---|
| CVEs | — |
| CVSS base score | 10.0 |
| Remediation | Addressed by remediation action A162 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 445/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 10.0. Severity rating 4 (derived from CVSS). |
| Rank position | Position 17 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:C/I:C/A:C — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #18 PostgreSQL Multiple Vulnerabilities (Aug 2025) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.155168

| | |
|---|---|
| CVEs | — |
| CVSS base score | 10.0 |
| Remediation | Addressed by remediation action A172 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 5432/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 10.0. Severity rating 4 (derived from CVSS). |
| Rank position | Position 18 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:C/I:C/A:C — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #19 TWiki < 4.2.4 Multiple XSS / Command Execution Vulnerabilities

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.800320

| | |
|---|---|
| CVEs | — |
| CVSS base score | 10.0 |
| Remediation | Addressed by remediation action A179 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 10.0. Severity rating 4 (derived from CVSS). |
| Rank position | Position 19 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:C/I:C/A:C — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #20 ProFTPD < 1.3.3c Multiple Vulnerabilities

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.801639

| | |
|---|---|
| CVEs | — |
| CVSS base score | 10.0 |
| Remediation | Addressed by remediation action A190 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default general |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 10.0. Severity rating 4 (derived from CVSS). |
| Rank position | Position 20 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:C/I:C/A:C — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #21 PHP 4.3.x < 5.2.7 Buffer Overflow Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.900185

| | |
|---|---|
| CVEs | — |
| CVSS base score | 10.0 |
| Remediation | Addressed by remediation action A2 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 10.0. Severity rating 4 (derived from CVSS). |
| Rank position | Position 21 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:C/I:C/A:C — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #22 jQuery End of Life (EOL) Detection - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.117149

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.9 |
| Remediation | Addressed by remediation action A283 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.9. Severity rating 4 (derived from CVSS). |
| Rank position | Position 22 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H — Attack vector: Network — Privileges required: Low — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #23 phpMyAdmin Code Injection and XSS Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100077

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A26 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 23 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #24 vsftpd Compromised Source Packages Backdoor Vulnerability - Active Check

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.103185

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A14 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 21/tcp, 6200/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 24 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #25 Samba Elevation of Privilege Vulnerability (CVE-2022-45141)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.104475

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A71 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 445/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 25 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #26 OpenBSD OpenSSH < 9.3p2 RCE Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.104869

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A297 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 22/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 26 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #27 PHP < 5.6.30, 7.x < 7.0.15, 7.1.x < 7.1.1 Multiple Vulnerabilities (Jan 2017) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.108052

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A89 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 27 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #28 PHP 'CVE-2019-13224' Use-After-Free Vulnerability - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.108633

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A93 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 28 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #29 PHP < 7.1.33, 7.2.x < 7.2.24, 7.3.x < 7.3.11 RCE Vulnerability - Version Check

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.108692

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A96 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 29 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #30 PHP < 5.2.5 Multiple Vulnerabilities

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.108866

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A2 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 30 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #31 PHP < 5.2.6 Multiple Vulnerabilities

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.108867

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A2 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 31 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #32 PostgreSQL < 10.6, 11.x < 11.1 SQL Injection Vulnerability - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.112429

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A98 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 5432/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 32 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #33 Apache HTTP Server <= 2.4.52 Multiple Vulnerabilities - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.113837

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A3 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 33 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #34 Apache HTTP Server < 2.4.60 Multiple Vulnerabilities - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.114682

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A3 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 34 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #35 PHP <= 7.1.5 Multiple DoS Vulnerabilities

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.117799

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A1 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 35 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #36 PHP < 7.0.12 RCE / DoS Vulnerability - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.117800

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A110 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 36 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #37 PHP <= 5.6.27 / 7.0.x <= 7.0.12 DoS Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.117802

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A1 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 37 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #38 PHP < 5.6.29, 7.0.x < 7.0.14 DoS Vulnerability - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.117803

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A111 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 38 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #39 Apache HTTP Server <= 2.4.51 Buffer Overflow Vulnerability - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.117856

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A3 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 39 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #40 phpMyAdmin < 4.8.6 SQL Injection Vulnerability (PMASA-2019-3) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.140207

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A115 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 40 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #41 PHP Multiple Vulnerabilities (Feb 2019) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.142048

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A119 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 41 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #42 ProFTPD <= 1.3.6 Arbitrary File Copy Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.142662

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A268 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default general |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 42 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #43 phpMyAdmin < 4.9.2 Multiple Vulnerabilities (PMASA-2019-5) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.143167

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A7 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 43 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #44 Apache Tomcat AJP RCE Vulnerability (Ghostcat) - Active Check

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.143545

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A264 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 8009/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 44 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #45 phpMyAdmin < 4.9.6, 5.x < 5.0.3 Multiple Vulnerabilities (PMASA-2020-5, PMASA-2020-6) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.144896

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A130 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 45 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #46 Apache HTTP Server < 2.4.49 Multiple Vulnerabilities - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.146725

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A3 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 46 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #47 PHP < 7.4.28, 8.0.x < 8.0.16, 8.1.x < 8.1.3 Security Update (Feb 2022) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.147657

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A151 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 47 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #48 Apache HTTP Server < 2.4.54 Multiple Vulnerabilities - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.148252

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A3 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 48 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #49 PHP < 7.4.33, 8.0.x < 8.0.25, 8.1.x < 8.1.12 Security Update - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.148830

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A154 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 49 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #50 PHP < 8.1.29, 8.2.x < 8.2.20, 8.3.x < 8.3.8 Multiple Vulnerabilities - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.152369

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A166 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 50 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #51 PHP < 8.1.31, 8.2.x < 8.2.26, 8.3.x < 8.3.14 Multiple Vulnerabilities - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.153495

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A167 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 51 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #52 PHP < 8.1.32, 8.2.x < 8.2.28 Multiple Vulnerabilities - Linux

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.154187

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A169 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 52 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #53 PHP < 8.0.30, 8.1.x < 8.1.22, 8.2.x < 8.2.9 Security Update - Linux

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.170529

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A178 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 53 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #54 PHP < 5.2.6 Multiple Vulnerabilities (Aug 2008)

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.800110

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A2 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 54 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #55 phpMyAdmin 2.11.x < 2.11.9.4 / 3.0.x < 3.1.3 Multiple Vulnerabilities

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.800381

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A180 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 55 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #56 PHP < 5.4.40, 5.5.x < 5.5.24, 5.6.x < 5.6.8 Multiple Vulnerabilities - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.805657

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A202 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 56 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #57 PostgreSQL Multiple Vulnerabilities (May 2015) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.805805

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A207 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 5432/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 57 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #58 PHP < 5.4.43, 5.5.x < 5.5.27, 5.6.x < 5.6.11 Multiple Vulnerabilities (Mar 2016) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.807507

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A212 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 58 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #59 PHP < 5.5.33, 5.6.x < 5.6.19 Multiple Vulnerabilities (Apr 2016) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.807807

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A215 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 59 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #60 PHP < 5.5.34, 5.6.x < 5.6.20, 7.x < 7.0.5 Multiple Vulnerabilities (Jul 2016) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.808199

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A216 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 60 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #61 PHP < 5.5.35, 5.6.x < 5.6.21, 7.x < 7.0.6 Multiple Vulnerabilities (Jul 2016) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.808603

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A217 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 61 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #62 PHP < 5.4.44, 5.5.x < 5.5.28, 5.6.x < 5.6.12 Multiple Vulnerabilities (Jul 2016) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.808604

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A218 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 62 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #63 PHP < 5.5.32, 5.6.x < 5.6.18, 7.x < 7.0.3 Multiple Vulnerabilities (Jul 2016) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.808607

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A219 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 63 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #64 PHP < 5.4.45, 5.5.x < 5.5.29, 5.6.x < 5.6.13 Multiple Vulnerabilities (Jul 2016) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.808617

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A223 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 64 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #65 PHP < 5.5.38, 5.6.x < 5.6.24, 7.0.x < 7.0.9 Multiple Vulnerabilities (Jul 2016) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.808634

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A226 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 65 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #66 PHP < 5.5.27, 5.6.x < 5.6.11 Arbitrary Code Execution Vulnerability (Aug 2016) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.808671

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A229 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 66 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #67 PHP < 5.6.7 DoS Vulnerability - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.808673

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A5 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 67 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #68 PHP < 5.4.42, 5.5.x < 5.5.26, 5.6.x < 5.6.10 Multiple Vulnerabilities (Aug 2016) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.808675

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A230 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 68 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #69 PHP < 5.5.37, 5.6.x < 5.6.23, 7.x < 7.0.8 Multiple Vulnerabilities (Aug 2016) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.808788

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A231 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 69 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #70 PHP < 5.5.37, 5.6.x < 5.6.23 Multiple Vulnerabilities (Aug 2016) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.808790

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A232 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 70 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #71 PHP < 5.6.26, 7.x < 7.0.11 Multiple Vulnerabilities (Sep 2016) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.809317

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A238 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 71 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #72 PHP < 5.6.25, 7.x < 7.0.10 Multiple Vulnerabilities (Sep 2016) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.809319

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A239 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 72 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #73 PHP < 5.6.26 DoS Vulnerability - Linux

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.809321

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A5 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 73 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #74 PHP < 5.6.27, 7.x < 7.0.12 Multiple DoS Vulnerabilities (Oct 2016) - Linux

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.809338

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A240 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 74 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #75 OpenSSH < 7.2 X11 Forwarding Security Bypass Vulnerability - Linux

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.810769

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A243 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 22/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 75 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #76 Apache HTTP Server Multiple Vulnerabilities (Jun 2017) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.811214

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A291 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 76 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #77 PHP < 5.6.31, 7.0.x < 7.0.21, 7.1.x < 7.1.7 Multiple Vulnerabilities (Jul 2017) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.811482

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A244 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 77 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #78 PHP < 5.6.28, 7.x < 7.0.13 Multiple Vulnerabilities (Nov 2016) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.811489

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A246 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 78 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #79 PHP 5.x < 5.6.34, 7.x < 7.0.28, 7.1.x < 7.1.15, 7.2.x < 7.2.3 Stack Buffer Overflow Vulnerability (Mar 2018) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.812821

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.8 |
| Remediation | Addressed by remediation action A253 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.8. Severity rating 4 (derived from CVSS). |
| Rank position | Position 79 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #80 PHP < 5.5.22, 5.6.x < 5.6.6 XXE Vulnerability - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.808615

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.6 |
| Remediation | Addressed by remediation action A222 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.6. Severity rating 4 (derived from CVSS). |
| Rank position | Position 80 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: Required — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #81 DistCC RCE Vulnerability (CVE-2004-2687)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.103553

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.3 |
| Remediation | Addressed by remediation action A64 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 3632/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.3. Severity rating 4 (derived from CVSS). |
| Rank position | Position 81 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:C/I:C/A:C — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #82 PHP < 5.2.14 Multiple Vulnerabilities

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.108861

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.3 |
| Remediation | Addressed by remediation action A2 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.3. Severity rating 4 (derived from CVSS). |
| Rank position | Position 82 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:C/I:C/A:C — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #83 PHP < 5.3.3 Multiple Vulnerabilities

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.108869

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.3 |
| Remediation | Addressed by remediation action A4 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.3. Severity rating 4 (derived from CVSS). |
| Rank position | Position 83 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:C/I:C/A:C — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #84 PHP 5.2.x < 5.2.12, 5.3.0 Buffer Overflow Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.801123

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.3 |
| Remediation | Addressed by remediation action A186 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.3. Severity rating 4 (derived from CVSS). |
| Rank position | Position 84 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:C/I:C/A:C — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #85 PHP < 7.2.27, 7.3.x < 7.3.14, 7.4.x < 7.4.2 Multiple Vulnerabilities (Jan 2020) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.143392

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.1 |
| Remediation | Addressed by remediation action A124 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.1. Severity rating 4 (derived from CVSS). |
| Rank position | Position 85 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #86 PHP < 5.5.31, 5.6.x < 5.6.17, 7.x < 7.0.2 Out of Bounds Read Memory Corruption Vulnerability (Mar 2016) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.807504

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.1 |
| Remediation | Addressed by remediation action A210 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.1. Severity rating 4 (derived from CVSS). |
| Rank position | Position 86 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #87 PHP < 5.5.31, 5.6.x < 5.6.17, 7.x < 7.0.2 DoS Vulnerability (Aug 2016) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.809139

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.1 |
| Remediation | Addressed by remediation action A236 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.1. Severity rating 4 (derived from CVSS). |
| Rank position | Position 87 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #88 Apache HTTP Server 'mod_auth_digest' Multiple Vulnerabilities - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.811237

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.1 |
| Remediation | Addressed by remediation action A292 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.1. Severity rating 4 (derived from CVSS). |
| Rank position | Position 88 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #89 ProFTPD < 1.3.3g RCE Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.103331

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.0 |
| Remediation | Addressed by remediation action A60 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default general |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.0. Severity rating 4 (derived from CVSS). |
| Rank position | Position 89 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:S/C:C/I:C/A:C — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #90 PostgreSQL Default Credentials (PostgreSQL Protocol)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.103552

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.0 |
| Remediation | Addressed by remediation action A63 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 5432/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.0. Severity rating 4 (derived from CVSS). |
| Rank position | Position 90 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:C/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #91 VNC Brute Force Login

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.106056

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.0 |
| Remediation | Addressed by remediation action A84 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 5900/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.0. Severity rating 4 (derived from CVSS). |
| Rank position | Position 91 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:C/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #92 Apache HTTP Server < 2.4.55 Multiple Vulnerabilities - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.149152

| | |
|---|---|
| CVEs | — |
| CVSS base score | 9.0 |
| Remediation | Addressed by remediation action A3 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 9.0. Severity rating 4 (derived from CVSS). |
| Rank position | Position 92 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #93 Samba Multiple Vulnerabilities (Jul 2022)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.104259

| | |
|---|---|
| CVEs | — |
| CVSS base score | 8.8 |
| Remediation | Addressed by remediation action A68 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 445/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 8.8. Severity rating 3 (derived from CVSS). |
| Rank position | Position 93 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: Low — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #94 Samba Buffer Overflow Vulnerability (CVE-2022-42898)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.104423

| | |
|---|---|
| CVEs | — |
| CVSS base score | 8.8 |
| Remediation | Addressed by remediation action A70 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 445/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 8.8. Severity rating 3 (derived from CVSS). |
| Rank position | Position 94 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: Low — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #95 ProFTPD < 1.3.7 Multiple Vulnerabilities

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.113645

| | |
|---|---|
| CVEs | — |
| CVSS base score | 8.8 |
| Remediation | Addressed by remediation action A101 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default general |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 8.8. Severity rating 3 (derived from CVSS). |
| Rank position | Position 95 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: Low — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #96 PHP < 8.1.30, 8.2.x < 8.2.24, 8.3.x < 8.3.12 Multiple Vulnerabilities - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.114787

| | |
|---|---|
| CVEs | — |
| CVSS base score | 8.8 |
| Remediation | Addressed by remediation action A103 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 8.8. Severity rating 3 (derived from CVSS). |
| Rank position | Position 96 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: Low — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #97 phpMyAdmin < 4.9.4, 5.x < 5.0.1 SQL Injection Vulnerability (PMASA-2020-1) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.143346

| | |
|---|---|
| CVEs | — |
| CVSS base score | 8.8 |
| Remediation | Addressed by remediation action A123 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 8.8. Severity rating 3 (derived from CVSS). |
| Rank position | Position 97 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: Low — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #98 phpMyAdmin <= 5.1.1 CSV Injection Vulnerability - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.144898

| | |
|---|---|
| CVEs | — |
| CVSS base score | 8.8 |
| Remediation | Addressed by remediation action A1 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 8.8. Severity rating 3 (derived from CVSS). |
| Rank position | Position 98 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: Required — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #99 Samba RCE Vulnerability (CVE-2021-44142)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.147554

| | |
|---|---|
| CVEs | — |
| CVSS base score | 8.8 |
| Remediation | Addressed by remediation action A149 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 445/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 8.8. Severity rating 3 (derived from CVSS). |
| Rank position | Position 99 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: Low — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #100 PHP < 7.4.30, 8.0.x < 8.0.20, 8.1.x < 8.1.7 Security Update (Jun 2022) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.148249

| | |
|---|---|
| CVEs | — |
| CVSS base score | 8.8 |
| Remediation | Addressed by remediation action A153 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 8.8. Severity rating 3 (derived from CVSS). |
| Rank position | Position 100 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: Low — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #101 PostgreSQL Multiple Vulnerabilities (Mar 2015) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.807518

| | |
|---|---|
| CVEs | — |
| CVSS base score | 8.8 |
| Remediation | Addressed by remediation action A213 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 5432/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 8.8. Severity rating 3 (derived from CVSS). |
| Rank position | Position 101 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: Low — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #102 PHP < 5.6.18, 7.x < 7.0.3 DoS Vulnerability (Jul 2016) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.808609

| | |
|---|---|
| CVEs | — |
| CVSS base score | 8.8 |
| Remediation | Addressed by remediation action A220 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 8.8. Severity rating 3 (derived from CVSS). |
| Rank position | Position 102 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: Required — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #103 PHP < 5.6.36, 7.x < 7.0.30, 7.1.x < 7.1.17, 7.2.x < 7.2.5 Multiple Vulnerabilities (May 2018) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.813160

| | |
|---|---|
| CVEs | — |
| CVSS base score | 8.8 |
| Remediation | Addressed by remediation action A254 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 8.8. Severity rating 3 (derived from CVSS). |
| Rank position | Position 103 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: Required — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #104 PHP < 5.5.36, 5.6.x < 5.6.22 Multiple Vulnerabilities (Aug 2016) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.808792

| | |
|---|---|
| CVEs | — |
| CVSS base score | 8.6 |
| Remediation | Addressed by remediation action A233 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 8.6. Severity rating 3 (derived from CVSS). |
| Rank position | Position 104 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #105 PHP < 5.5.36, 5.6.x < 5.6.22, 7.x < 7.0.7 Multiple Vulnerabilities (Aug 2016) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.808794

| | |
|---|---|
| CVEs | — |
| CVSS base score | 8.6 |
| Remediation | Addressed by remediation action A234 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 8.6. Severity rating 3 (derived from CVSS). |
| Rank position | Position 105 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #106 PostgreSQL Multiple Security Vulnerabilities

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100645

| | |
|---|---|
| CVEs | — |
| CVSS base score | 8.5 |
| Remediation | Addressed by remediation action A43 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 5432/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 8.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 106 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:S/C:C/I:C/A:C — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #107 OpenSSH Multiple Vulnerabilities

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.806052

| | |
|---|---|
| CVEs | — |
| CVSS base score | 8.5 |
| Remediation | Addressed by remediation action A307 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 22/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 8.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 107 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:N/A:C — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #108 PostgreSQL Code Injection and Denial of Service Vulnerabilities - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.808665

| | |
|---|---|
| CVEs | — |
| CVSS base score | 8.3 |
| Remediation | Addressed by remediation action A227 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 5432/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 8.3. Severity rating 3 (derived from CVSS). |
| Rank position | Position 108 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:H — Attack vector: Network — Privileges required: Low — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #109 PHP < 8.2.30, 8.3.x < 8.3.29, 8.4.x < 8.4.16 Multiple Vulnerabilities - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.156071

| | |
|---|---|
| CVEs | — |
| CVSS base score | 8.2 |
| Remediation | Addressed by remediation action A177 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 8.2. Severity rating 3 (derived from CVSS). |
| Rank position | Position 109 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #110 Samba Multiple Vulnerabilities (Dec 2022)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.104476

| | |
|---|---|
| CVEs | — |
| CVSS base score | 8.1 |
| Remediation | Addressed by remediation action A72 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 445/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 8.1. Severity rating 3 (derived from CVSS). |
| Rank position | Position 110 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #111 PHP < 8.0.28, 8.1.x < 8.1.16, 8.2.x < 8.2.3 Security Update - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.104541

| | |
|---|---|
| CVEs | — |
| CVSS base score | 8.1 |
| Remediation | Addressed by remediation action A74 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 8.1. Severity rating 3 (derived from CVSS). |
| Rank position | Position 111 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #112 Samba 3.0.0 < 4.13.14, 4.14.0 < 4.14.10, 4.15.0 < 4.15.2 Multiple Vulnerabilities

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.147124

| | |
|---|---|
| CVEs | — |
| CVSS base score | 8.1 |
| Remediation | Addressed by remediation action A145 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 445/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 8.1. Severity rating 3 (derived from CVSS). |
| Rank position | Position 112 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N — Attack vector: Network — Privileges required: Low — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #113 PostgreSQL < 9.6.24, 10.x < 10.19, 11.x < 11.14, 12.x < 12.9, 13.x < 13.5, 14.x < 14.1 Multiple Vulnerabilities - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.147148

| | |
|---|---|
| CVEs | — |
| CVSS base score | 8.1 |
| Remediation | Addressed by remediation action A146 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 5432/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 8.1. Severity rating 3 (derived from CVSS). |
| Rank position | Position 113 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #114 PHP < 5.6.24, 7.x <= 7.0.8 Multiple Vulnerabilities (Jul 2016) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.808628

| | |
|---|---|
| CVEs | — |
| CVSS base score | 8.1 |
| Remediation | Addressed by remediation action A224 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 8.1. Severity rating 3 (derived from CVSS). |
| Rank position | Position 114 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #115 Apache HTTP Server Man-in-the-Middle Attack Vulnerability (Jul 2016) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.808632

| | |
|---|---|
| CVEs | — |
| CVSS base score | 8.1 |
| Remediation | Addressed by remediation action A225 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 8.1. Severity rating 3 (derived from CVSS). |
| Rank position | Position 115 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #116 phpMyAdmin < 4.9.5, 5.x < 5.0.2 Multiple SQL Injection Vulnerabilities (PMASA-2020-2, PMASA-2020-3, PMASA-2020-4) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.112715

| | |
|---|---|
| CVEs | — |
| CVSS base score | 8.0 |
| Remediation | Addressed by remediation action A99 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 8.0. Severity rating 3 (derived from CVSS). |
| Rank position | Position 116 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: Low — User interaction: Required — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #117 Samba < 3.4.0 Remote Code Execution Vulnerability (CVE-2012-0870)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.150728

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.9 |
| Remediation | Addressed by remediation action A161 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 445/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.9. Severity rating 3 (derived from CVSS). |
| Rank position | Position 117 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:A/AC:M/Au:N/C:C/I:C/A:C — Attack vector: Adjacent network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #118 Samba 'mount.cifs' Utility Symlink Attack Local Privilege Escalation Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100623

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.8 |
| Remediation | Addressed by remediation action A40 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 445/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.8. Severity rating 3 (derived from CVSS). |
| Rank position | Position 118 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H — Attack vector: Local — Privileges required: Low — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #119 PHP < 8.0.27, 8.1.x < 8.1.14, 8.2.x < 8.2.1 Security Update - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.149069

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.8 |
| Remediation | Addressed by remediation action A155 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.8. Severity rating 3 (derived from CVSS). |
| Rank position | Position 119 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:N/I:N/A:C — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #120 ProFTPD < 1.3.8c Access Control Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.155384

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.8 |
| Remediation | Addressed by remediation action A174 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default general |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.8. Severity rating 3 (derived from CVSS). |
| Rank position | Position 120 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:C/I:N/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #121 OpenSSH <= 7.2p2 Privilege Escalation Vulnerability (May 2016)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.807574

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.8 |
| Remediation | Addressed by remediation action A296 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 22/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.8. Severity rating 3 (derived from CVSS). |
| Rank position | Position 121 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H — Attack vector: Local — Privileges required: Low — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #122 OpenSSH < 7.4 Multiple Vulnerabilities (Jan 2017) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.8103256

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.8 |
| Remediation | Addressed by remediation action A241 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 22/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.8. Severity rating 3 (derived from CVSS). |
| Rank position | Position 122 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H — Attack vector: Local — Privileges required: Low — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #123 PostgreSQL SQLi Vulnerability (Feb 2025) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.154018

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.6 |
| Remediation | Addressed by remediation action A168 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 5432/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.6. Severity rating 3 (derived from CVSS). |
| Rank position | Position 123 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:H/Au:N/C:C/I:C/A:C — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #124 phpMyAdmin BLOB Streaming Multiple Input Validation Vulnerabilities

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100078

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A27 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 124 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #125 rsh Unencrypted Cleartext Login

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100080

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A275 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 514/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 125 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #126 phpMyAdmin 'CVE-2009-1285' Configuration File PHP Code Injection Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100144

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A304 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 126 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #127 PHP <= 5.2.10 Interruptions and Calltime Arbitrary Code Execution Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100252

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A1 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 127 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #128 Apache HTTP Server < 2.4.58 'mod_macro' Out-of-bounds Read Vulnerability - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100272

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A3 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 128 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #129 phpMyAdmin Unspecified SQL Injection and Cross Site Scripting Vulnerabilities

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100307

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A31 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 129 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #130 PHP < 5.3.1 Multiple Vulnerabilities

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100359

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A33 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 130 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #131 PHP < 5.2.13 Multiple Vulnerabilities

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100511

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A2 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 131 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #132 PHP Multiple Buffer Overflow Vulnerabilities

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100583

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A39 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 132 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #133 PHP 5.2.x < 5.2.14, 5.3.x < 5.3.3 Multiple RCE Vulnerabilities

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100631

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A41 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 133 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #134 Samba < 3.3.13 'SMB1 Packet Chaining' Unspecified Remote Memory Corruption Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100680

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A45 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 445/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 134 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #135 PHP 'SplObjectStorage' Unserializer Arbitrary Code Execution Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100684

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A46 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 135 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #136 Samba < 3.5.5 SID Parsing Remote Buffer Overflow Vulnerability

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100803

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A51 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 445/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 136 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #137 PHP < 5.3.6 Remote Integer Overflow Vulnerability

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.103113

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A4 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 137 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #138 PHP < 5.3.13, 5.4.x < 5.4.3 Multiple Vulnerabilities - Active Check

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.103482

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A280 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 138 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #139 Samba Multiple Vulnerabilities (Jul 2023)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.104872

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A77 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 445/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 139 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #140 Test HTTP dangerous methods

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.10498

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A303 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 140 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #141 OpenSSH 'schnorr.c' Remote Memory Corruption Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.105001

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A79 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 22/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 141 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #142 ProFTPD < 1.3.6b, 1.3.7rc < 1.3.7rc2 DoS Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.107734

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A85 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default general |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 142 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #143 Apache HTTP Server OPTIONS Memory Leak Vulnerability (Optionsbleed) - Version Check

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.108252

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A91 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 143 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #144 PHP 5.x < 5.6.39, 7.x < 7.0.33, 7.1.x < 7.1.26, 7.2.x < 7.2.14 DoS Vulnerability - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.108505

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A92 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 144 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #145 FTP Brute Force Logins With Default Credentials Reporting

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.108718

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A17 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 21/tcp, 2121/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 145 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #146 PHP 'CVE-2017-7189' Improper Input Validation Vulnerability - Linux

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.108874

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A1 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 146 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #147 PHP 5.x < 5.4.4 Memory Leak Vulnerability

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.117788

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A109 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 147 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #148 Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSH, D(HE)ater)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.117839

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A263 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 22/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 148 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #149 Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.117840

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A20 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 25/tcp, 5432/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 149 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #150 Java RMI Server Insecure Default Configuration RCE Vulnerability - Active Check

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.140051

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A270 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 1099/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 150 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #151 ProFTPD < 1.3.6 Multiple Vulnerabilities

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.143205

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A121 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default general |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 151 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #152 ProFTPD < 1.3.6c CRL Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.143206

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A122 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default general |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 152 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #153 PHP < 7.2.28 Multiple Vulnerabilities (Feb 2020) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.143541

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A6 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 153 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #154 PHP < 7.2.30, 7.3 < 7.3.17, 7.4 < 7.4.5 DoS Vulnerability (Apr 2020) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.143722

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A126 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 154 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #155 PHP < 7.3.27, 7.4.x < 7.4.15, 8.0.x < 8.0.2 NULL Deference Vulnerability (Feb 2021) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.145323

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A132 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 155 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #156 phpMyAdmin < 4.9.10, 5.x < 5.1.3 Information Disclosure Vulnerability - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.147786

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A152 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 156 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #157 OpenSSH <= 5.6 Improper Authentication Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.150632

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A157 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 22/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 157 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #158 Samba 3.0.6 <= 3.0.23d Multiple Vulnerabilities

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.150723

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A12 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 445/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 158 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #159 Apache HTTP Server < 2.4.59 Multiple Vulnerabilities - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.152039

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A3 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 159 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #160 PHP < 8.1.33, 8.2.x < 8.2.29, 8.3.x < 8.3.23, 8.4.x < 8.4.10 Multiple Vulnerabilities - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.154869

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A171 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 160 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #161 PHP 5.2.11, 5.3.x < 5.3.1 Multiple Vulnerabilities (Dec 2009)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.801060

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A185 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 161 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #162 EasyPHP Webserver <= 12.1 Multiple Vulnerabilities - Active Check

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.803189

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A1 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 162 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #163 PHP < 5.3.28, 5.4.x < 5.4.23, 5.5.x < 5.5.7 RCE Vulnerability (Dec 2013)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.804174

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A194 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 163 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #164 PHP 5.2.x < 5.2.7 Buffer Overflow Vulnerability (Jan 2015)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.805410

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A2 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 164 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #165 PHP < 5.5.21, 5.6.x < 5.6.5 Multiple DoS Vulnerabilities (Jan 2015)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.805412

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A198 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 165 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #166 PHP < 5.6.5 Multiple Vulnerabilities (Jan 2015)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.805413

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A5 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 166 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #167 PHP Out of Bounds Read Vulnerability (Jan 2015)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.805414

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A199 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 167 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #168 PHP < 5.4.39, 5.5.x < 5.5.23, 5.6.x < 5.6.7 Multiple Vulnerabilities - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.805651

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A201 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 168 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #169 PHP < 5.4.41, 5.5.x < 5.5.25, 5.6.x < 5.6.9 Multiple Vulnerabilities - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.805660

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A204 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 169 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #170 PHP < 5.4.38, 5.5.x < 5.5.22, 5.6.x < 5.6.6 Multiple RCE Vulnerabilities (Jul 2015) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.805685

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A205 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 170 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #171 PHP < 5.5.24, 5.6.x < 5.6.8 DoS Vulnerability - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.805687

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A206 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 171 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #172 PHP 5.4.44, 5.5.x < 5.5.28, 5.6.x < 5.6.12 Multiple Vulnerabilities (Mar 2016) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.807503

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A209 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 172 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #173 Samba Badlock Critical Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.807646

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A214 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 445/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 173 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: None — User interaction: Required — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #174 PHP < 5.6.12 Multiple DoS Vulnerabilities - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.808611

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A5 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 174 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #175 PHP < 5.6.0 DoS Vulnerability - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.808669

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A5 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 175 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #176 OpenSSH < 7.3 DoS and User Enumeration Vulnerabilities - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.809154

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A237 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 22/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 176 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #177 PostgreSQL Multiple Information Disclosure Vulnerabilities (May 2017) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.810990

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A300 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 5432/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 177 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #178 PHP < 5.6.31, 7.x < 7.0.17, 7.1.x < 7.1.3 DoS Vulnerability (Jul 2017) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.811487

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A245 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 178 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #179 PHP < 5.6.31 DoS Vulnerability - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.811490

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A5 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 179 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #180 Apache HTTP Server 'Whitespace Defects' Multiple Vulnerabilities

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.812033

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A290 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 180 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #181 PHP < 5.6.32, 7.x < 7.0.24, 7.1.x < 7.1.11 Heap Based Buffer Overflow Vulnerability - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.812073

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A249 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 181 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #182 PHP < 5.5.32, 5.6.x < 5.6.18, 7.x < 7.0.3 Privilege Escalation Vulnerability - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.812512

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A250 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 182 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #183 PHP Multiple Heap Buffer Overflow and Information Disclosure Vulnerabilities (Aug 2018) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.813901

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A258 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 183 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #184 PHP Security Bypass and File Writing Vulnerabilities (Dec 2008)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.900184

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A2 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 184 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #185 Samba 3.0.0 <= 3.0.29 Buffer Overflow Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.90028

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A267 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 445/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 185 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #186 ProFTPD 1.3.1 - 1.3.2rc2 SQLi Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.900507

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A8 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default general |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 186 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #187 PHP Multiple Vulnerabilities (Sep 2009)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.900871

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A2 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 187 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #188 The rlogin service is running

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.901202

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A13 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 513/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 188 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #189 PHP < 5.3.7 Use After Free Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.902356

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.5 |
| Remediation | Addressed by remediation action A4 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.5. Severity rating 3 (derived from CVSS). |
| Rank position | Position 189 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #190 SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.105042

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.4 |
| Remediation | Addressed by remediation action A82 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 5432/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.4. Severity rating 3 (derived from CVSS). |
| Rank position | Position 190 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #191 OpenBSD OpenSSH <= 8.6 Command Injection Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.113736

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.4 |
| Remediation | Addressed by remediation action A1 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 22/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.4. Severity rating 3 (derived from CVSS). |
| Rank position | Position 191 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:A/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H — Attack vector: Adjacent network — Privileges required: Low — User interaction: Required — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #192 PostgreSQL < 9.5.23, 9.6.x < 9.6.19, 10.x < 10.14, 11.x < 11.9, 12.x < 12.4 Search Path Vulnerability - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.144709

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.3 |
| Remediation | Addressed by remediation action A129 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 5432/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.3. Severity rating 3 (derived from CVSS). |
| Rank position | Position 192 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H — Attack vector: Local — Privileges required: Low — User interaction: Required — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #193 PHP < 5.4.45, 5.5.x < 5.5.29, 5.6.x < 5.6.13 RCE Vulnerability (Mar 2016) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.807505

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.3 |
| Remediation | Addressed by remediation action A211 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.3. Severity rating 3 (derived from CVSS). |
| Rank position | Position 193 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #194 Samba 3.0.0 <= 4.3.2 Bypass File-Access Restrictions Vulnerability (CVE-2015-5252)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.150746

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.2 |
| Remediation | Addressed by remediation action A164 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 445/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.2. Severity rating 3 (derived from CVSS). |
| Rank position | Position 194 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #195 Apache HTTP Server 'mod_proxy_http.c' Denial Of Service Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.800827

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.1 |
| Remediation | Addressed by remediation action A183 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.1. Severity rating 3 (derived from CVSS). |
| Rank position | Position 195 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:N/I:N/A:C — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #196 Apache HTTP Server 'mod_deflate' Denial Of Service Vulnerability (Jul 2009)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.800837

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.1 |
| Remediation | Addressed by remediation action A184 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.1. Severity rating 3 (derived from CVSS). |
| Rank position | Position 196 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:N/I:N/A:C — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #197 PHP < 5.4.44, 5.5.x < 5.5.28, 5.6.x < 5.6.12, 7.x < 7.0.4 DoS and Information Disclosure Vulnerability - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.808666

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.1 |
| Remediation | Addressed by remediation action A228 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.1. Severity rating 3 (derived from CVSS). |
| Rank position | Position 197 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H — Attack vector: Local — Privileges required: Low — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #198 Samba Server 'SMB1' Memory Information Leak Vulnerability (CVE-2017-12163)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.811905

| | |
|---|---|
| CVEs | — |
| CVSS base score | 7.1 |
| Remediation | Addressed by remediation action A247 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 445/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 7.1. Severity rating 3 (derived from CVSS). |
| Rank position | Position 198 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N — Attack vector: Adjacent network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #199 Apache HTTP Server Privilege Escalation Vulnerability (Mar 2012) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.147056

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.9 |
| Remediation | Addressed by remediation action A143 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.9. Severity rating 2 (derived from CVSS). |
| Rank position | Position 199 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:L/AC:M/Au:N/C:C/I:C/A:C — Attack vector: Local — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #200 PostgreSQL Multiple Security Vulnerabilities (Sep 2009)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100273

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.8 |
| Remediation | Addressed by remediation action A29 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 5432/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.8. Severity rating 2 (derived from CVSS). |
| Rank position | Position 200 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #201 PHP 5.x < 5.3.4 Improper Input Validation Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100901

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.8 |
| Remediation | Addressed by remediation action A4 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.8. Severity rating 2 (derived from CVSS). |
| Rank position | Position 201 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #202 Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.103935

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.8 |
| Remediation | Addressed by remediation action A65 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 25/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.8. Severity rating 2 (derived from CVSS). |
| Rank position | Position 202 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #203 PHP Heap Use-After-Free Vulnerability (Sep 2019) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.108635

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.8 |
| Remediation | Addressed by remediation action A94 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.8. Severity rating 2 (derived from CVSS). |
| Rank position | Position 203 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #204 PHP Multiple Vulnerabilities (Sep 2019) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.108637

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.8 |
| Remediation | Addressed by remediation action A95 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.8. Severity rating 2 (derived from CVSS). |
| Rank position | Position 204 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #205 PHP < 5.3.4 Multiple Vulnerabilities

Band 5 | no CVE, non-trivial severity | Plugin 1.3.6.1.4.1.25623.1.0.108870

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.8 |
| Remediation | Addressed by remediation action A4 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.8. Severity rating 2 (derived from CVSS). |
| Rank position | Position 205 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #206 OpenBSD OpenSSH <= 7.9 Multiple Vulnerabilities

Band 5 | no CVE, non-trivial severity | Plugin 1.3.6.1.4.1.25623.1.0.117786

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.8 |
| Remediation | Addressed by remediation action A108 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 22/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.8. Severity rating 2 (derived from CVSS). |
| Rank position | Position 206 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N — Attack vector: Network — Privileges required: None — User interaction: Required — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #207 Apache HTTP Server Multiple Vulnerabilities (Sep 2014) - Linux

Band 5 | no CVE, non-trivial severity | Plugin 1.3.6.1.4.1.25623.1.0.147048

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.8 |
| Remediation | Addressed by remediation action A138 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.8. Severity rating 2 (derived from CVSS). |
| Rank position | Position 207 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #208 Samba Symlink Race Vulnerability (CVE-2021-20316)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.147401

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.8 |
| Remediation | Addressed by remediation action A148 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 445/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.8. Severity rating 2 (derived from CVSS). |
| Rank position | Position 208 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N — Attack vector: Network — Privileges required: Low — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #209 TWiki Cross-Site Request Forgery Vulnerability (Sep 2010)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.801281

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.8 |
| Remediation | Addressed by remediation action A309 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.8. Severity rating 2 (derived from CVSS). |
| Rank position | Position 209 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #210 PHP < 5.2.15, 5.3.x < 5.3.4 DoS Vulnerabilities

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.801586

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.8 |
| Remediation | Addressed by remediation action A189 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.8. Severity rating 2 (derived from CVSS). |
| Rank position | Position 210 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #211 PHP < 5.5.2 Session Fixation Vulnerability (Aug 2013)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.803737

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.8 |
| Remediation | Addressed by remediation action A191 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.8. Severity rating 2 (derived from CVSS). |
| Rank position | Position 211 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #212 PHP < 5.4.40, 5.5.x < 5.5.24, 5.6.x < 5.6.8 Improper Input Validation Vulnerability (Jun 2015) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.805658

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.8 |
| Remediation | Addressed by remediation action A203 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.8. Severity rating 2 (derived from CVSS). |
| Rank position | Position 212 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #213 PHP < 5.5.30, 5.6.x < 5.6.14 Multiple DoS Vulnerabilities - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.806649

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.8 |
| Remediation | Addressed by remediation action A208 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.8. Severity rating 2 (derived from CVSS). |
| Rank position | Position 213 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #214 ProFTPD < 1.3.2rc3 CSRF Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.900133

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.8 |
| Remediation | Addressed by remediation action A8 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default general |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.8. Severity rating 2 (derived from CVSS). |
| Rank position | Position 214 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #215 Samba Security Feature Bypass Vulnerability (CVE-2020-17049)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.117760

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.6 |
| Remediation | Addressed by remediation action A106 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 445/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.6. Severity rating 2 (derived from CVSS). |
| Rank position | Position 215 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H — Attack vector: Network — Privileges required: High — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #216 PostgreSQL NULL Character CA SSL Certificate Validation Security Bypass Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100400

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.5 |
| Remediation | Addressed by remediation action A34 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 5432/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.5. Severity rating 2 (derived from CVSS). |
| Rank position | Position 216 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:S/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #217 PostgreSQL 'bitsubstr' Buffer Overflow Vulnerability

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100470

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.5 |
| Remediation | Addressed by remediation action A35 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 5432/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.5. Severity rating 2 (derived from CVSS). |
| Rank position | Position 217 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:S/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #218 PostgreSQL 'intarray' Module 'gettoken()' Buffer Overflow Vulnerability

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.103054

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.5 |
| Remediation | Addressed by remediation action A56 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 5432/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.5. Severity rating 2 (derived from CVSS). |
| Rank position | Position 218 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:S/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #219 phpMyAdmin Bookmark Security Bypass Vulnerability

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.103076

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.5 |
| Remediation | Addressed by remediation action A57 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.5. Severity rating 2 (derived from CVSS). |
| Rank position | Position 219 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:S/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #220 PHP < 7.4.31, 8.0.x < 8.0.24, 8.1.x < 8.1.11 Security Update - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.104331

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.5 |
| Remediation | Addressed by remediation action A69 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.5. Severity rating 2 (derived from CVSS). |
| Rank position | Position 220 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N — Attack vector: Network — Privileges required: None — User interaction: Required — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #221 Samba File Truncation Vulnerability (CVE-2023-3347)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.104957

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.5 |
| Remediation | Addressed by remediation action A78 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 445/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.5. Severity rating 2 (derived from CVSS). |
| Rank position | Position 221 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N — Attack vector: Network — Privileges required: Low — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #222 PHP < 7.3.31, 7.4.x < 7.4.24, 8.0.x < 8.0.11 Security Update (Sep 2021) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.117694

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.5 |
| Remediation | Addressed by remediation action A105 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.5. Severity rating 2 (derived from CVSS). |
| Rank position | Position 222 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N — Attack vector: Network — Privileges required: None — User interaction: Required — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #223 Samba Security Vulnerability (CVE-2019-10218)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.117772

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.5 |
| Remediation | Addressed by remediation action A107 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 445/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.5. Severity rating 2 (derived from CVSS). |
| Rank position | Position 223 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N — Attack vector: Network — Privileges required: None — User interaction: Required — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #224 OpenBSD OpenSSH < 9.6 Multiple Vulnerabilities (Terrapin Attack)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.118572

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.5 |
| Remediation | Addressed by remediation action A112 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 22/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.5. Severity rating 2 (derived from CVSS). |
| Rank position | Position 224 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #225 phpMyAdmin < 4.9.0 CSRF Vulnerability (PMASA-2019-4) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.142499

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.5 |
| Remediation | Addressed by remediation action A7 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.5. Severity rating 2 (derived from CVSS). |
| Rank position | Position 225 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N — Attack vector: Network — Privileges required: None — User interaction: Required — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #226 phpMyAdmin < 4.9.1 CSRF Vulnerability - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.142897

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.5 |
| Remediation | Addressed by remediation action A7 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.5. Severity rating 2 (derived from CVSS). |
| Rank position | Position 226 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N — Attack vector: Network — Privileges required: None — User interaction: Required — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #227 PHP < 7.2.26 Multiple Vulnerabilities (Dec 2019) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.143276

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.5 |
| Remediation | Addressed by remediation action A6 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.5. Severity rating 2 (derived from CVSS). |
| Rank position | Position 227 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #228 PostgreSQL < 9.4.26, 9.5.x < 9.5.21, 9.6.x < 9.6.17, 10.x < 10.12, 11.x < 11.7, 12.x < 12.2 Authorization Check Vulnerability - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.143610

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.5 |
| Remediation | Addressed by remediation action A125 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 5432/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.5. Severity rating 2 (derived from CVSS). |
| Rank position | Position 228 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N — Attack vector: Network — Privileges required: Low — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #229 PHP < 7.2.34, 7.3 < 7.3.23, 7.4 < 7.4.11 Multiple Vulnerabilities (Oct 2020) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.144694

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.5 |
| Remediation | Addressed by remediation action A128 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.5. Severity rating 2 (derived from CVSS). |
| Rank position | Position 229 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #230 Samba < 4.14.8 DoS Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.146864

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.5 |
| Remediation | Addressed by remediation action A135 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 445/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.5. Severity rating 2 (derived from CVSS). |
| Rank position | Position 230 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H — Attack vector: Network — Privileges required: Low — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #231 OpenSSH 4.4 < 4.9 Permission, Privileges and Access Controls Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.150633

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.5 |
| Remediation | Addressed by remediation action A158 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 22/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.5. Severity rating 2 (derived from CVSS). |
| Rank position | Position 231 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:S/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #232 Samba 'fd_open_atomic infinite loop' DoS Vulnerability (CVE-2017-9461)

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.811083

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.5 |
| Remediation | Addressed by remediation action A301 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 445/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.5. Severity rating 2 (derived from CVSS). |
| Rank position | Position 232 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H — Attack vector: Network — Privileges required: Low — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #233 PHP 5.x < 7.1.20, 7.2.x < 7.2.8, 7.3.0alpha1 < 7.3.0alpha3 DoS Vulnerability - Linux

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.812520

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.5 |
| Remediation | Addressed by remediation action A251 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.5. Severity rating 2 (derived from CVSS). |
| Rank position | Position 233 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H — Attack vector: Network — Privileges required: Low — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #234 PHP 5.x < 5.3.9 Security Bypass Vulnerability

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.103464

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.4 |
| Remediation | Addressed by remediation action A4 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.4. Severity rating 2 (derived from CVSS). |
| Rank position | Position 234 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #235 OpenSSH <= 7.2p1 Xauth Command Injection Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.105581

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.4 |
| Remediation | Addressed by remediation action A295 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 22/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.4. Severity rating 2 (derived from CVSS). |
| Rank position | Position 235 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N — Attack vector: Network — Privileges required: Low — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #236 phpMyAdmin 3.x < 3.3.10.3, 3.4.x < 3.4.3.2 Multiple Vulnerabilities (PMASA-2011-9, PMASA-2011-12) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.108242

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.4 |
| Remediation | Addressed by remediation action A90 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.4. Severity rating 2 (derived from CVSS). |
| Rank position | Position 236 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:N/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #237 PHP 5.2.x < 5.2.14, 5.3.x < 5.3.3 Multiple Information Disclosure Vulnerabilities

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.801359

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.4 |
| Remediation | Addressed by remediation action A187 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.4. Severity rating 2 (derived from CVSS). |
| Rank position | Position 237 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #238 Anonymous FTP Login Reporting

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.900600

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.4 |
| Remediation | Addressed by remediation action A279 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 21/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.4. Severity rating 2 (derived from CVSS). |
| Rank position | Position 238 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:P/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #239 PHP 4.x, 5.2.6 DoS Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.900925

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.4 |
| Remediation | Addressed by remediation action A2 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.4. Severity rating 2 (derived from CVSS). |
| Rank position | Position 239 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:N/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #240 phpMyAdmin <= 4.8.2 XSS Vulnerability (PMASA-2018-5) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.113255

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.1 |
| Remediation | Addressed by remediation action A100 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.1. Severity rating 2 (derived from CVSS). |
| Rank position | Position 240 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N — Attack vector: Network — Privileges required: None — User interaction: Required — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #241 jQuery < 3.0.0 XSS Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.141635

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.1 |
| Remediation | Addressed by remediation action A116 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.1. Severity rating 2 (derived from CVSS). |
| Rank position | Position 241 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N — Attack vector: Network — Privileges required: None — User interaction: Required — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #242 jQuery < 1.9.0 XSS Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.141636

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.1 |
| Remediation | Addressed by remediation action A10 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.1. Severity rating 2 (derived from CVSS). |
| Rank position | Position 242 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N — Attack vector: Network — Privileges required: None — User interaction: Required — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #243 TWiki < 6.1.0 XSS Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.141830

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.1 |
| Remediation | Addressed by remediation action A118 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.1. Severity rating 2 (derived from CVSS). |
| Rank position | Position 243 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N — Attack vector: Network — Privileges required: None — User interaction: Required — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #244 jQuery < 3.4.0 Object Extensions Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.142314

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.1 |
| Remediation | Addressed by remediation action A120 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.1. Severity rating 2 (derived from CVSS). |
| Rank position | Position 244 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N — Attack vector: Network — Privileges required: None — User interaction: Required — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #245 jQuery 1.2 < 3.5.0 XSS Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.143812

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.1 |
| Remediation | Addressed by remediation action A11 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.1. Severity rating 2 (derived from CVSS). |
| Rank position | Position 245 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N — Attack vector: Network — Privileges required: None — User interaction: Required — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #246 jQuery 1.0.3 < 3.5.0 XSS Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.143813

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.1 |
| Remediation | Addressed by remediation action A11 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.1. Severity rating 2 (derived from CVSS). |
| Rank position | Position 246 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N — Attack vector: Network — Privileges required: None — User interaction: Required — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #247 jQuery < 1.9.0 XSS Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.143968

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.1 |
| Remediation | Addressed by remediation action A10 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.1. Severity rating 2 (derived from CVSS). |
| Rank position | Position 247 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N — Attack vector: Network — Privileges required: None — User interaction: Required — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #248 Apache HTTP Server CRLF Injection Vulnerability (Dec 2016) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.147044

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.1 |
| Remediation | Addressed by remediation action A136 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.1. Severity rating 2 (derived from CVSS). |
| Rank position | Position 248 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N — Attack vector: Network — Privileges required: None — User interaction: Required — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #249 PHP < 5.4.38, 5.5.x < 5.5.22, 5.6.x < 5.6.6 XSS Vulnerability (Aug 2016) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.809137

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.1 |
| Remediation | Addressed by remediation action A235 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.1. Severity rating 2 (derived from CVSS). |
| Rank position | Position 249 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N — Attack vector: Network — Privileges required: None — User interaction: Required — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #250 PHP < 5.6.33, 7.x < 7.0.27, 7.1.x < 7.1.13, 7.2.x < 7.2.1 Multiple Vulnerabilities - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.812735

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.1 |
| Remediation | Addressed by remediation action A252 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.1. Severity rating 2 (derived from CVSS). |
| Rank position | Position 250 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N — Attack vector: Network — Privileges required: None — User interaction: Required — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #251 phpMyAdmin Cross-Site Scripting Vulnerability (PMASA-2018-3) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.813451

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.1 |
| Remediation | Addressed by remediation action A256 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.1. Severity rating 2 (derived from CVSS). |
| Rank position | Position 251 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N — Attack vector: Network — Privileges required: None — User interaction: Required — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #252 Samba < 3.0.37, 3.1.x < 3.2.15, 3.3.x < 3.3.8, 3.4.x < 3.4.2 Multiple Vulnerabilities

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100306

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.0 |
| Remediation | Addressed by remediation action A30 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 445/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 252 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:S/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #253 PostgreSQL PL/Perl and PL/Tcl Local Privilege Escalation Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100843

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.0 |
| Remediation | Addressed by remediation action A52 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 5432/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 253 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:S/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #254 Samba 3.0.0 <= 3.0.25rc3 MS-RPC Remote Shell Command Execution Vulnerability - Active Check

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.108011

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.0 |
| Remediation | Addressed by remediation action A86 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 445/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 254 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:S/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #255 Samba 3.0.0 <= 3.0.25rc3 MS-RPC Remote Shell Command Execution Vulnerability - Version Check

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.108012

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.0 |
| Remediation | Addressed by remediation action A87 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 445/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 255 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:S/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #256 TWiki CSRF Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.800400

| | |
|---|---|
| CVEs | — |
| CVSS base score | 6.0 |
| Remediation | Addressed by remediation action A182 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 6.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 256 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:S/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #257 SSL/TLS: Report Weak Cipher Suites

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.103440

> Severity data varies across affected instances: the scan did not report the same severity or CVSS score for every occurrence of this issue. Review the per-instance detail before treating them as equivalent. Observed severity ratings: 0, 2. Observed CVSS base scores: 5.9. The single CVSS shown for this issue is the representative value from its highest-priority occurrence.

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.9 |
| Remediation | Addressed by remediation action A15 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 25/tcp, 5432/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.9. Severity rating 2 (derived from CVSS). |
| Rank position | Position 257 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #258 SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.111012

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.9 |
| Remediation | Addressed by remediation action A18 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 25/tcp, 5432/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.9. Severity rating 2 (derived from CVSS). |
| Rank position | Position 258 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #259 PHP < 7.3.29 Multiple Vulnerabilities (Jul 2021) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.117524

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.9 |
| Remediation | Addressed by remediation action A104 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.9. Severity rating 2 (derived from CVSS). |
| Rank position | Position 259 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #260 Samba 4.1 < 4.17.1 Improper Authentication (CVE-2021-20251)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.126184

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.9 |
| Remediation | Addressed by remediation action A113 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 445/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.9. Severity rating 2 (derived from CVSS). |
| Rank position | Position 260 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #261 ProFTPD < 1.3.8b OpenSSH Terrapin Attack

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.155383

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.9 |
| Remediation | Addressed by remediation action A173 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default general |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.9. Severity rating 2 (derived from CVSS). |
| Rank position | Position 261 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #262 PHP < 5.5.28, 5.6.x < 5.6.12 DoS Vulnerability (Jul 2016) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.808613

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.9 |
| Remediation | Addressed by remediation action A221 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.9. Severity rating 2 (derived from CVSS). |
| Rank position | Position 262 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #263 ProFTPD < 1.3.2b, 1.3.3 - 1.3.3.rc1 SSL Certificate Validation Bypass Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100316

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.8 |
| Remediation | Addressed by remediation action A32 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default general |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.8. Severity rating 2 (derived from CVSS). |
| Rank position | Position 263 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:N/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #264 PHP Directory Traversal Vulnerability (Apr 2012)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.103486

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.8 |
| Remediation | Addressed by remediation action A62 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.8. Severity rating 2 (derived from CVSS). |
| Rank position | Position 264 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:N/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #265 OpenSSH Certificate Validation Security Bypass Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.105004

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.8 |
| Remediation | Addressed by remediation action A81 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 22/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.8. Severity rating 2 (derived from CVSS). |
| Rank position | Position 265 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:P/I:P/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #266 HTTP Debugging Methods (TRACE/TRACK) Enabled

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.11213

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.8 |
| Remediation | Addressed by remediation action A97 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.8. Severity rating 2 (derived from CVSS). |
| Rank position | Position 266 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:P/I:P/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #267 PHP < 8.1.28, 8.2.x < 8.2.18, 8.3.x < 8.3.6 Security Update (GHSA-h746-cjrr-wfmr) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.152118

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.8 |
| Remediation | Addressed by remediation action A165 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.8. Severity rating 2 (derived from CVSS). |
| Rank position | Position 267 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:P/I:P/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #268 Samba Format String Vulnerability

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.900685

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.8 |
| Remediation | Addressed by remediation action A261 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 445/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.8. Severity rating 2 (derived from CVSS). |
| Rank position | Position 268 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:P/I:P/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #269 PostgreSQL 'RESET ALL' Unauthorized Access Vulnerability

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100648

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.5 |
| Remediation | Addressed by remediation action A44 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 5432/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.5. Severity rating 2 (derived from CVSS). |
| Rank position | Position 269 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:S/C:P/I:P/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #270 PHP < 8.0.22, 8.1.x < 8.1.9 Security Update - Linux

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.104644

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.5 |
| Remediation | Addressed by remediation action A76 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.5. Severity rating 2 (derived from CVSS). |
| Rank position | Position 270 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H — Attack vector: Local — Privileges required: Low — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #271 ProFTPD < 1.3.5e, 1.3.6 < 1.3.6rc5 Local Security Bypass Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.810731

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.5 |
| Remediation | Addressed by remediation action A242 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default general |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.5. Severity rating 2 (derived from CVSS). |
| Rank position | Position 271 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N — Attack vector: Local — Privileges required: Low — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #272 PHP < 7.2.29 Multiple Vulnerabilities (Mar 2020) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.143615

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.4 |
| Remediation | Addressed by remediation action A6 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.4. Severity rating 2 (derived from CVSS). |
| Rank position | Position 272 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:L — Attack vector: Network — Privileges required: None — User interaction: Required — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #273 PostgreSQL DoS Vulnerability (Feb 2025) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.154470

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.4 |
| Remediation | Addressed by remediation action A170 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 5432/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.4. Severity rating 2 (derived from CVSS). |
| Rank position | Position 273 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:H/Au:N/C:N/I:N/A:C — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #274 PostgreSQL Multiple Vulnerabilities (Nov 2025) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.155797

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.4 |
| Remediation | Addressed by remediation action A176 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 5432/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.4. Severity rating 2 (derived from CVSS). |
| Rank position | Position 274 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:H/Au:N/C:N/I:N/A:C — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #275 phpinfo() Output Reporting (HTTP)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.11229

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.3 |
| Remediation | Addressed by remediation action A269 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.3. Severity rating 2 (derived from CVSS). |
| Rank position | Position 275 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #276 Weak Host Key Algorithm(s) (SSH)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.117687

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.3 |
| Remediation | Addressed by remediation action A272 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 22/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.3. Severity rating 2 (derived from CVSS). |
| Rank position | Position 276 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N — Attack vector: Adjacent network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #277 OpenSSH Information Disclosure Vulnerability (CVE-2016-20012)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.117777

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.3 |
| Remediation | Addressed by remediation action A1 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 22/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.3. Severity rating 2 (derived from CVSS). |
| Rank position | Position 277 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #278 PHP < 7.2.31, 7.3 < 7.3.18, 7.4 < 7.4.6 Multiple DoS Vulnerabilities (May 2020) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.143913

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.3 |
| Remediation | Addressed by remediation action A127 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.3. Severity rating 2 (derived from CVSS). |
| Rank position | Position 278 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #279 PHP < 7.3.26, 7.4.x < 7.4.14, 8.0.x < 8.0.1 Filter Vulnerability (Jan 2021) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.145114

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.3 |
| Remediation | Addressed by remediation action A131 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.3. Severity rating 2 (derived from CVSS). |
| Rank position | Position 279 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #280 PHP < 7.3.33, 7.4.x < 7.4.26, 8.0.x < 8.0.13 Security Update (Nov 2021) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.147187

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.3 |
| Remediation | Addressed by remediation action A147 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.3. Severity rating 2 (derived from CVSS). |
| Rank position | Position 280 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #281 SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.150710

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.3 |
| Remediation | Addressed by remediation action A22 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 25/tcp, 5432/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.3. Severity rating 2 (derived from CVSS). |
| Rank position | Position 281 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N — Attack vector: Adjacent network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #282 Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.150713

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.3 |
| Remediation | Addressed by remediation action A273 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 22/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.3. Severity rating 2 (derived from CVSS). |
| Rank position | Position 282 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N — Attack vector: Adjacent network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #283 OpenSSH < 7.1p2 DoS Vulnerability (Jan 2016)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.806671

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.3 |
| Remediation | Addressed by remediation action A294 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 22/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.3. Severity rating 2 (derived from CVSS). |
| Rank position | Position 283 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #284 OpenSSH < 7.6 'sftp-server' Security Bypass Vulnerability - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.812051

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.3 |
| Remediation | Addressed by remediation action A248 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 22/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.3. Severity rating 2 (derived from CVSS). |
| Rank position | Position 284 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #285 OpenSSH < 7.8 User Enumeration Vulnerability - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.813864

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.3 |
| Remediation | Addressed by remediation action A257 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 22/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.3. Severity rating 2 (derived from CVSS). |
| Rank position | Position 285 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #286 vsftpd < 2.3.5 Buffer Overflow Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.103362

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.1 |
| Remediation | Addressed by remediation action A61 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 21/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.1. Severity rating 2 (derived from CVSS). |
| Rank position | Position 286 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:H/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #287 Apache HTTP Server Log Escape Filtering Vulnerability (Jul 2013) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.147051

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.1 |
| Remediation | Addressed by remediation action A140 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.1. Severity rating 2 (derived from CVSS). |
| Rank position | Position 287 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:H/Au:N/C:P/I:P/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #288 Check if Mailserver answer to VRFY and EXPN requests

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100072

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A276 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 25/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 288 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:N/I:N/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #289 PHP <= 5.2.8 Multiple Vulnerabilities

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100146

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A2 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 289 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:N/I:N/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #290 PHP 5.3.1 Multiple DoS Vulnerabilities

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100529

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A37 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 290 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:N/I:N/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #291 /doc directory browsable

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.10056

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A302 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 291 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:N/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #292 PHP 4.4.x < 4.4.9, 5.2.x < 5.2.8 DoS Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100582

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A38 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 292 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:N/I:N/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #293 Samba < 3.4.8, 3.5.x < 3.5.2 Multiple Remote DoS Vulnerabilities

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100644

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A42 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 445/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 293 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:N/I:N/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #294 PHP 5.x < 5.3.3 Information Disclosure Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100695

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A4 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 294 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:N/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #295 Apache HTTP Server Multiple Remote Denial of Service Vulnerabilities

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100725

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A47 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 295 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:N/I:N/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #296 PHP 5.2.x < 5.2.14, 5.3.x < 5.3.3 Multiple Vulnerabilities

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100726

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A48 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 296 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:N/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #297 PHP 'mb_strcut()' Function Information Disclosure Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100898

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A53 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 297 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:N/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #298 PHP 5.2.x < 5.2.17, 5.3.x < 5.3.5 DoS Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.103020

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A55 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 298 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:N/I:N/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #299 Samba < 3.5.7 'FD_SET' Memory Corruption Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.103095

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A58 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 445/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 299 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:N/I:N/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #300 awiki <= 20100125 Multiple LFI Vulnerabilities - Active Check

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.103210

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A1 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 300 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:N/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #301 OpenSSH Denial of Service Vulnerability

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.103939

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A67 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 22/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 301 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:N/I:N/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #302 SSL/TLS: Certificate Expired

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.103955

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A23 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 25/tcp, 5432/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 302 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:N/I:P/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #303 OpenBSD OpenSSH < 9.2 Unspecified Vulnerability

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.104512

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A73 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 22/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 303 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:N/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #304 OpenBSD OpenSSH < 9.3 Unspecified Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.104635

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A75 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 22/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 304 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:N/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #305 vsftpd < 3.0.3 Security Bypass Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.108045

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A88 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 21/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 305 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:N/I:P/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #306 Enabled Directory Listing/Indexing Detection (HTTP)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.111074

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A278 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 306 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:N/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #307 SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.117761

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A25 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 25/tcp, 5432/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 307 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:N/I:N/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #308 PHP < 7.3.28, 7.4.x < 7.4.18 IMAP Header Injection Vulnerability (Apr 2021) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.145869

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A133 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 308 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:N/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #309 PHP < 7.3.30, 7.4.x < 7.4.23, 8.0.x < 8.0.10 Security Update (Aug 2021) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.146584

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A134 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 309 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:N/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #310 Apache HTTP Server Multiple Vulnerabilities (Mar 2014) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.147047

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A137 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 310 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:N/I:N/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #311 Samba 3.0.1 <= 3.0.22 DoS Vulnerability (CVE-2006-3403)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.150722

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A159 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 445/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 311 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:N/I:N/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #312 Samba 3.0.0 <= 4.0.7 DoS Vulnerability (CVE-2013-4124)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.150732

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A163 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 445/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 312 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:N/I:N/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #313 Apache HTTP Server < 2.4.64 Multiple Vulnerabilities - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.154909

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A3 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 313 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:N/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #314 ProFTPD < 1.3.9 DoS Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.155385

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A175 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default general |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 314 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:N/I:N/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #315 QWikiwiki directory traversal vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.16100

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A1 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 315 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:N/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #316 PHP DoS Vulnerability (Apr 2009)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.800393

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A181 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 316 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:N/I:N/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #317 Samba < 3.0.32 winbind Daemon DoS Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.800711

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A12 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 445/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 317 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:N/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #318 PHP 'ext/imap/php_imap.c' Use After Free DoS Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.801583

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A293 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 318 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:N/I:N/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #319 PHP < 5.3.4 Multiple Security Bypass Vulnerabilities

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.801585

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A4 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 319 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:N/I:P/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #320 PHP < 5.2.15 Security Bypass Vulnerability

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.801731

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A2 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 320 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:N/I:P/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #321 PHP < 5.3.29, 5.4.x < 5.4.24, 5.5.x < 5.5.8 RCE Vulnerability

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.804160

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A193 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 321 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:N/I:N/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #322 PHP 'open_basedir' Security Bypass Vulnerability

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.804241

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A1 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 322 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:N/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #323 PHP 5.x < 5.4.29, 5.5.x < 5.5.13 Multiple DoS Vulnerabilities (Jun 2014)

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.804639

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A196 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 323 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:N/I:N/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #324 Apache HTTP Server 'mod_lua' Denial of Service Vulnerability -01 (May 2015)

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.805616

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A200 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 324 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:N/I:N/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #325 PHP 5.x < 5.2.9 Memory Information Disclosure Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.900186

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A2 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 325 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:P/I:N/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #326 Apache HTTP Server 'mod_proxy_ftp' Module Command Injection Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.900842

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A262 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 326 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:N/I:P/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #327 PHP <= 5.3.0 DoS Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.900993

| | |
|---|---|
| CVEs | — |
| CVSS base score | 5.0 |
| Remediation | Addressed by remediation action A1 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 5.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 327 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:N/C:N/I:N/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #328 Apache HTTP Server 'Options' and 'AllowOverride' Directives Security Bypass Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100211

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.9 |
| Remediation | Addressed by remediation action A28 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.9. Severity rating 2 (derived from CVSS). |
| Rank position | Position 328 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:L/AC:L/Au:N/C:N/I:N/A:C — Attack vector: Local — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #329 OpenSSH 'child_set_env()' Function Security Bypass Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.105003

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.9 |
| Remediation | Addressed by remediation action A80 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 22/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.9. Severity rating 2 (derived from CVSS). |
| Rank position | Position 329 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:N — Attack vector: Network — Privileges required: Low — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #330 Cleartext Transmission of Sensitive Information via HTTP

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.108440

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.8 |
| Remediation | Addressed by remediation action A277 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.8. Severity rating 2 (derived from CVSS). |
| Rank position | Position 330 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:A/AC:L/Au:N/C:P/I:P/A:N — Attack vector: Adjacent network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #331 Telnet Unencrypted Cleartext Login

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.108522

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.8 |
| Remediation | Addressed by remediation action A281 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 23/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.8. Severity rating 2 (derived from CVSS). |
| Rank position | Position 331 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:A/AC:L/Au:N/C:P/I:P/A:N — Attack vector: Adjacent network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #332 FTP Unencrypted Cleartext Login

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.108528

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.8 |
| Remediation | Addressed by remediation action A21 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 21/tcp, 2121/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.8. Severity rating 2 (derived from CVSS). |
| Rank position | Position 332 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:A/AC:L/Au:N/C:P/I:P/A:N — Attack vector: Adjacent network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #333 VNC Server Unencrypted Data Transmission

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.108529

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.8 |
| Remediation | Addressed by remediation action A282 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 5900/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.8. Severity rating 2 (derived from CVSS). |
| Rank position | Position 333 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:A/AC:L/Au:N/C:P/I:P/A:N — Attack vector: Adjacent network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #334 Samba 'mtab' Lock File Handling Local DoS Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.103283

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.7 |
| Remediation | Addressed by remediation action A59 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 445/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.7. Severity rating 2 (derived from CVSS). |
| Rank position | Position 334 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H — Attack vector: Local — Privileges required: Low — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #335 PHP < 5.6.35, 7.x < 7.0.29, 7.1.x < 7.1.16, 7.2.x < 7.2.4 Security Bypass Vulnerability (May 2018) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.813162

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.7 |
| Remediation | Addressed by remediation action A255 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.7. Severity rating 2 (derived from CVSS). |
| Rank position | Position 335 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N — Attack vector: Local — Privileges required: Low — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #336 Apache HTTP Server Multiple Vulnerabilities (Jan 2012) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.147057

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.6 |
| Remediation | Addressed by remediation action A9 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.6. Severity rating 2 (derived from CVSS). |
| Rank position | Position 336 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:L/AC:L/Au:N/C:P/I:P/A:P — Attack vector: Local — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #337 Samba <= 3.4.5 'mount.cifs' Utility Local Privilege Escalation Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100476

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.4 |
| Remediation | Addressed by remediation action A36 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 445/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.4. Severity rating 2 (derived from CVSS). |
| Rank position | Position 337 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:L/AC:M/Au:N/C:P/I:P/A:P — Attack vector: Local — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #338 PHP < 5.2.10 JPEG Image Processing DoS Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100581

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.3 |
| Remediation | Addressed by remediation action A2 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.3. Severity rating 2 (derived from CVSS). |
| Rank position | Position 338 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:N/I:N/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #339 phpMyAdmin Multiple Cross Site Scripting Vulnerabilities

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100761

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.3 |
| Remediation | Addressed by remediation action A49 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.3. Severity rating 2 (derived from CVSS). |
| Rank position | Position 339 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:N/I:P/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #340 phpMyAdmin Debug Backtrace Cross Site Scripting Vulnerability

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100775

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.3 |
| Remediation | Addressed by remediation action A50 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.3. Severity rating 2 (derived from CVSS). |
| Rank position | Position 340 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:N/I:P/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #341 phpMyAdmin Database Search Cross Site Scripting Vulnerability

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100939

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.3 |
| Remediation | Addressed by remediation action A54 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.3. Severity rating 2 (derived from CVSS). |
| Rank position | Position 341 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:N/I:P/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #342 Weak Encryption Algorithm(s) Supported (SSH)

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.105611

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.3 |
| Remediation | Addressed by remediation action A271 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 22/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.3. Severity rating 2 (derived from CVSS). |
| Rank position | Position 342 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:P/I:N/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #343 PostgreSQL < 9.5.25, 9.6.x < 9.6.21, 10.x < 10.16, 11.x < 11.11, 12.x < 12.6, 13.x < 13.2 Information Disclosure Vulnerability - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.113791

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.3 |
| Remediation | Addressed by remediation action A102 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 5432/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.3. Severity rating 2 (derived from CVSS). |
| Rank position | Position 343 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N — Attack vector: Network — Privileges required: Low — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #344 SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.117274

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.3 |
| Remediation | Addressed by remediation action A19 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 25/tcp, 5432/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.3. Severity rating 2 (derived from CVSS). |
| Rank position | Position 344 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:N/I:P/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #345 Apache HTTP Server < 2.4.66 SSI Vulnerability - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.125564

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.3 |
| Remediation | Addressed by remediation action A3 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.3. Severity rating 2 (derived from CVSS). |
| Rank position | Position 345 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:N/I:P/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #346 jQuery < 1.6.3 XSS Vulnerability

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.141637

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.3 |
| Remediation | Addressed by remediation action A117 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.3. Severity rating 2 (derived from CVSS). |
| Rank position | Position 346 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:N/I:P/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #347 Apache HTTP Server DoS Vulnerability (Jul 2013) - Linux

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.147050

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.3 |
| Remediation | Addressed by remediation action A139 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.3. Severity rating 2 (derived from CVSS). |
| Rank position | Position 347 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:N/I:N/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #348 Apache HTTP Server Multiple Vulnerabilities (Feb 2013) - Linux

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.147052

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.3 |
| Remediation | Addressed by remediation action A141 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.3. Severity rating 2 (derived from CVSS). |
| Rank position | Position 348 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:N/I:P/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #349 Apache HTTP Server XSS Vulnerability (Sep 2012) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.147055

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.3 |
| Remediation | Addressed by remediation action A142 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.3. Severity rating 2 (derived from CVSS). |
| Rank position | Position 349 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:N/I:P/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #350 Apache HTTP Server DoS Vulnerability (May 2011) - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.147060

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.3 |
| Remediation | Addressed by remediation action A144 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.3. Severity rating 2 (derived from CVSS). |
| Rank position | Position 350 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:N/I:N/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #351 Samba Information Disclosure Vulnerability (CVE-2021-44141)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.147555

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.3 |
| Remediation | Addressed by remediation action A150 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 445/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.3. Severity rating 2 (derived from CVSS). |
| Rank position | Position 351 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N — Attack vector: Network — Privileges required: Low — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #352 PHP < 8.0.29, 8.1.x < 8.1.20, 8.2.x < 8.2.7 Security Update - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.149760

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.3 |
| Remediation | Addressed by remediation action A156 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.3. Severity rating 2 (derived from CVSS). |
| Rank position | Position 352 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N — Attack vector: Network — Privileges required: Low — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #353 phpMyAdmin SQL bookmark XSS Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.800595

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.3 |
| Remediation | Addressed by remediation action A299 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.3. Severity rating 2 (derived from CVSS). |
| Rank position | Position 353 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:N/I:P/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #354 phpMyAdmin Setup Script Request Cross Site Scripting Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.801286

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.3 |
| Remediation | Addressed by remediation action A308 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.3. Severity rating 2 (derived from CVSS). |
| Rank position | Position 354 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:N/I:P/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #355 PHP 5.2.x < 5.2.15, 5.3.x < 5.3.4 Multiple Vulnerabilities

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.801547

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.3 |
| Remediation | Addressed by remediation action A188 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.3. Severity rating 2 (derived from CVSS). |
| Rank position | Position 355 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:N/I:N/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #356 phpMyAdmin 'error.php' Cross Site Scripting Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.801660

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.3 |
| Remediation | Addressed by remediation action A1 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.3. Severity rating 2 (derived from CVSS). |
| Rank position | Position 356 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:N/I:P/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #357 PHP < 5.3.22, 5.4.x < 5.4.12 SOAP Parser Multiple Information Disclosure Vulnerabilities

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.803764

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.3 |
| Remediation | Addressed by remediation action A192 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.3. Severity rating 2 (derived from CVSS). |
| Rank position | Position 357 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:P/I:N/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #358 PHP < 5.4.32, 5.5.x < 5.5.16 DoS Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.804292

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.3 |
| Remediation | Addressed by remediation action A195 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.3. Severity rating 2 (derived from CVSS). |
| Rank position | Position 358 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:N/I:N/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #359 SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.805142

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.3 |
| Remediation | Addressed by remediation action A197 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 25/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.3. Severity rating 2 (derived from CVSS). |
| Rank position | Position 359 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:N/I:P/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #360 OpenSSH Security Bypass Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.806049

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.3 |
| Remediation | Addressed by remediation action A306 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 22/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.3. Severity rating 2 (derived from CVSS). |
| Rank position | Position 360 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:N/I:P/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #361 Apache HTTP Server 'mod_proxy_ftp' Wildcard Characters XSS Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.900107

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.3 |
| Remediation | Addressed by remediation action A259 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.3. Severity rating 2 (derived from CVSS). |
| Rank position | Position 361 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:N/I:P/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #362 Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.902830

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.3 |
| Remediation | Addressed by remediation action A305 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 80/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.3. Severity rating 2 (derived from CVSS). |
| Rank position | Position 362 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:M/Au:N/C:P/I:N/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #363 PostgreSQL Conversion Encoding Remote DoS Vulnerability (Mar 2009)

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.100157

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.0 |
| Remediation | Addressed by remediation action A298 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 5432/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 363 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:S/C:N/I:N/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #364 OpenSSH <= 5.8 Multiple DoS Vulnerabilities

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.103937

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.0 |
| Remediation | Addressed by remediation action A66 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 22/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 364 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:S/C:N/I:N/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #365 SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.105880

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.0 |
| Remediation | Addressed by remediation action A24 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 25/tcp, 5432/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 365 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:H/Au:N/C:P/I:P/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #366 SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

Band 5 no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.106223

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.0 |
| Remediation | Addressed by remediation action A16 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 25/tcp, 5432/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 366 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:H/Au:N/C:P/I:P/A:N — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #367 OpenBSD OpenSSH < 9.1 Multiple Vulnerabilities

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.127244

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.0 |
| Remediation | Addressed by remediation action A114 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 22/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 367 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:A/AC:H/Au:S/C:P/I:P/A:P — Attack vector: Adjacent network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #368 ProFTPD < 1.3.2rc3 DoS Vulnerability

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.801640

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.0 |
| Remediation | Addressed by remediation action A8 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default general |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.0. Severity rating 2 (derived from CVSS). |
| Rank position | Position 368 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:S/C:N/I:N/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## #369 PostgreSQL 'CVE-2009-0922' Denial of Service Vulnerability - Linux

**Band 5** no CVE, non-trivial severity Plugin 1.3.6.1.4.1.25623.1.0.900480

| | |
|---|---|
| CVEs | — |
| CVSS base score | 4.0 |
| Remediation | Addressed by remediation action A260 |
| Affected hosts (1) | **172.18.0.18** metasploitable2.greenbone-community-edition_default 5432/tcp |
| Scoring rationale | Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. CVSS 4.0. Severity rating 2 (derived from CVSS). Ranked above SSL/TLS: Report Weak Cipher Suites (CVSS 5.9, no KEV match) because a finding with real severity outweighs informational noise. |
| Rank position | Position 369 of 369 within band, ordered by CVSS descending, then severity rating, then finding identifier. |

CVSS vector: AV:N/AC:L/Au:S/C:N/I:N/A:P — Attack vector: Network — Privileges required: Not encoded in CVSS v2 — User interaction: Not encoded in CVSS v2 — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

## Low or informational findings (reference only)

90 issues fall in the report's lowest band, low or informational: any finding the bands above do not match. Full detail (CVSS, scoring rationale, affected hosts, ports) is unchanged in the report's underlying data; this table is a compact index, not a call to action.

| # | Issue | Plugin ID | Hosts | Remediation |
|---|---|---|---|---|
| 370 | SSL/TLS: 'DHE_EXPORT' MITM Security Bypass Vulnerability (LogJam) | 1.3.6.1.4.1.25623.1.0.805188 | 1 | A325 |
| 371 | PHP <= 5.6.0 'PEAR' Symlink Attack Vulnerability | 1.3.6.1.4.1.25623.1.0.117252 | 1 | A331 |
| 372 | PHP < 7.2.33, 7.3 < 7.3.21, 7.4 < 7.4.9 DoS Vulnerability (Aug 2020) - Linux | 1.3.6.1.4.1.25623.1.0.144365 | 1 | A321 |
| 373 | Samba Symlink Directory Traversal Vulnerability (Feb 2010) | 1.3.6.1.4.1.25623.1.0.100488 | 1 | A312 |
| 374 | openssh-server Forced Command Handling Information Disclosure Vulnerability | 1.3.6.1.4.1.25623.1.0.103503 | 1 | A316 |
| 375 | PostgreSQL Hash Table Integer Overflow Vulnerability | 1.3.6.1.4.1.25623.1.0.902139 | 1 | A327 |
| 376 | SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE) | 1.3.6.1.4.1.25623.1.0.802087 | 1 | A310 |
| 377 | Samba 'etc/mtab' File Appending Local DoS Vulnerability | 1.3.6.1.4.1.25623.1.0.103298 | 1 | A314 |
| 378 | OpenSSH CBC Mode Information Disclosure Vulnerability | 1.3.6.1.4.1.25623.1.0.100153 | 1 | A332 |
| 379 | Weak MAC Algorithm(s) Supported (SSH) | 1.3.6.1.4.1.25623.1.0.105610 | 1 | A328 |
| 380 | PHP < 5.2.8 XSS Vulnerability | 1.3.6.1.4.1.25623.1.0.800334 | 1 | A2 |
| 381 | TCP Timestamps Information Disclosure | 1.3.6.1.4.1.25623.1.0.80091 | 1 | A324 |
| 382 | Apache HTTP Server 'mod_proxy_ftp' Module DoS Vulnerability | 1.3.6.1.4.1.25623.1.0.900841 | 1 | A326 |
| 383 | Samba Share Escape Vulnerability (CVE-2021-43566) | 1.3.6.1.4.1.25623.1.0.117876 | 1 | A318 |
| 384 | OpenBSD OpenSSH < 10.1 Multiple Vulnerabilities | 1.3.6.1.4.1.25623.1.0.119134 | 1 | A319 |
| 385 | PostgreSQL Low Cost Function Information Disclosure Vulnerability | 1.3.6.1.4.1.25623.1.0.100158 | 1 | A311 |
| 386 | Samba < 3.5.11 'client/mount.cifs.c' Remote DoS Vulnerability | 1.3.6.1.4.1.25623.1.0.100499 | 1 | A313 |
| 387 | ICMP Timestamp Reply Information Disclosure | 1.3.6.1.4.1.25623.1.0.103190 | 1 | A330 |
| 388 | OpenSSH 'ssh-keysign.c' Local Information Disclosure Vulnerability | 1.3.6.1.4.1.25623.1.0.105002 | 1 | A317 |
| 389 | PHP < 4.4.5, 5.1.x < 5.1.7, 5.2.x < 5.2.6 DoS Vulnerability | 1.3.6.1.4.1.25623.1.0.800373 | 1 | A323 |
| 390 | Apache HTTP Server 'ap_pregsub()' Function Local Denial of Service Vulnerability | 1.3.6.1.4.1.25623.1.0.103333 | 1 | A329 |
| 391 | OpenSSH < 5.1 Exposure of Sensitive Information to an Unauthorized Actor Vulnerability | 1.3.6.1.4.1.25623.1.0.150648 | 1 | A322 |
| 392 | Telnet Service Detection | 1.3.6.1.4.1.25623.1.0.100074 | 1 | A1 |

| # | Issue | Plugin ID | Hosts | Remediation |
|---|---|---|---|---|
| 393 | PostgreSQL Detection (TCP) | 1.3.6.1.4.1.25623.1.0.100151 | 1 | A1 |
| 394 | MariaDB / Oracle MySQL Detection (MySQL Protocol) | 1.3.6.1.4.1.25623.1.0.100152 | 1 | A1 |
| 395 | SSH Protocol Versions Supported | 1.3.6.1.4.1.25623.1.0.100259 | 1 | A1 |
| 396 | FTP Banner Detection | 1.3.6.1.4.1.25623.1.0.10092 | 1 | A1 |
| 397 | HTTP Server type and version | 1.3.6.1.4.1.25623.1.0.10107 | 1 | A1 |
| 398 | SMB NativeLanMan | 1.3.6.1.4.1.25623.1.0.102011 | 1 | A1 |
| 399 | SMTP Server type and version | 1.3.6.1.4.1.25623.1.0.10263 | 1 | A1 |
| 400 | SSH Server type and version | 1.3.6.1.4.1.25623.1.0.10267 | 1 | A1 |
| 401 | Telnet Banner Reporting | 1.3.6.1.4.1.25623.1.0.10281 | 1 | A1 |
| 402 | SSL/TLS: SMTP 'STARTTLS' Command Detection | 1.3.6.1.4.1.25623.1.0.103118 | 1 | A1 |
| 403 | SSL/TLS: Certificate - Self-Signed Certificate Detection | 1.3.6.1.4.1.25623.1.0.103140 | 1 | A1 |
| 404 | SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN | 1.3.6.1.4.1.25623.1.0.103141 | 1 | A1 |
| 405 | Services | 1.3.6.1.4.1.25623.1.0.10330 | 1 | A1 |
| 406 | VNC Server and Protocol Version Detection (TCP) | 1.3.6.1.4.1.25623.1.0.10342 | 1 | A315 |
| 407 | SSL/TLS: Report Non Weak Cipher Suites | 1.3.6.1.4.1.25623.1.0.103441 | 1 | A1 |
| 408 | SSL/TLS: Collect and Report Certificate Details | 1.3.6.1.4.1.25623.1.0.103692 | 1 | A1 |
| 409 | SMB log in | 1.3.6.1.4.1.25623.1.0.10394 | 1 | A1 |
| 410 | SSL/TLS: PostgreSQL SSL/TLS Support Detection (PostgreSQL Protocol) | 1.3.6.1.4.1.25623.1.0.105013 | 1 | A1 |
| 411 | SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites | 1.3.6.1.4.1.25623.1.0.105018 | 1 | A1 |
| 412 | SSH Protocol Algorithms Supported | 1.3.6.1.4.1.25623.1.0.105565 | 1 | A1 |
| 413 | SSL/TLS: Version Detection | 1.3.6.1.4.1.25623.1.0.105782 | 1 | A1 |
| 414 | RMI Registry Service Detection | 1.3.6.1.4.1.25623.1.0.105839 | 1 | A1 |
| 415 | OS Detection Consolidation and Reporting | 1.3.6.1.4.1.25623.1.0.105937 | 1 | A1 |
| 416 | Apache JServ Protocol (AJP) v1.3 Detection (TCP) | 1.3.6.1.4.1.25623.1.0.108082 | 1 | A1 |
| 417 | RPC Portmapper Service Detection (TCP) | 1.3.6.1.4.1.25623.1.0.108090 | 1 | A1 |
| 418 | Service Detection with 'BINARY' Request | 1.3.6.1.4.1.25623.1.0.108204 | 1 | A1 |
| 419 | Unknown OS and Service Banner Reporting | 1.3.6.1.4.1.25623.1.0.108441 | 1 | A1 |
| 420 | Hostname Determination Reporting | 1.3.6.1.4.1.25623.1.0.108449 | 1 | A1 |
| 421 | rsh Service Detection | 1.3.6.1.4.1.25623.1.0.108478 | 1 | A1 |
| 422 | SMB Login Successful For Authenticated Checks | 1.3.6.1.4.1.25623.1.0.108539 | 1 | A1 |
| 423 | SSL/TLS: FTP Missing Support For AUTH TLS | 1.3.6.1.4.1.25623.1.0.108553 | 1 | A1 |
| 424 | OpenSSH Detection Consolidation | 1.3.6.1.4.1.25623.1.0.108577 | 1 | A1 |

| # | Issue | Plugin ID | Hosts | Remediation |
|---|---|---|---|---|
| 425 | HTTP Server Banner Enumeration | 1.3.6.1.4.1.25623.1.0.108708 | 1 | A1 |
| 426 | SMB/CIFS Server Detection | 1.3.6.1.4.1.25623.1.0.11011 | 1 | A1 |
| 427 | SSL/TLS: Hostname discovery from server certificate | 1.3.6.1.4.1.25623.1.0.111010 | 1 | A1 |
| 428 | Web Application Scanning Consolidation / Info Reporting | 1.3.6.1.4.1.25623.1.0.111038 | 1 | A1 |
| 429 | vsftpd FTP Server Detection (FTP) | 1.3.6.1.4.1.25623.1.0.111050 | 1 | A1 |
| 430 | Postfix SMTP Server Detection (SMTP) | 1.3.6.1.4.1.25623.1.0.111086 | 1 | A1 |
| 431 | Obtain list of all port mapper registered programs via RPC | 1.3.6.1.4.1.25623.1.0.11111 | 1 | A1 |
| 432 | IRC Server Banner Detection | 1.3.6.1.4.1.25623.1.0.11156 | 1 | A1 |
| 433 | HTTP Security Headers Detection | 1.3.6.1.4.1.25623.1.0.112081 | 1 | A1 |
| 434 | rexec Detection | 1.3.6.1.4.1.25623.1.0.113763 | 1 | A1 |
| 435 | Apache HTTP Server Detection Consolidation | 1.3.6.1.4.1.25623.1.0.117232 | 1 | A1 |
| 436 | SSL/TLS: Safe/Secure Renegotiation Support Status | 1.3.6.1.4.1.25623.1.0.117757 | 1 | A1 |
| 437 | SSL/TLS: Untrusted Certificate Detection | 1.3.6.1.4.1.25623.1.0.117764 | 1 | A1 |
| 438 | PQC Key Exchange (KEX) Algorithm(s) Missing (SSH) | 1.3.6.1.4.1.25623.1.0.119214 | 1 | A320 |
| 439 | DistCC Detection | 1.3.6.1.4.1.25623.1.0.12638 | 1 | A1 |
| 440 | PostgreSQL Detection Consolidation | 1.3.6.1.4.1.25623.1.0.128025 | 1 | A1 |
| 441 | SMBv1 Enabled - Active Check | 1.3.6.1.4.1.25623.1.0.140151 | 1 | A1 |
| 442 | IP Forwarding Enabled - Active Check | 1.3.6.1.4.1.25623.1.0.147205 | 1 | A1 |
| 443 | jQuery Detection Consolidation | 1.3.6.1.4.1.25623.1.0.150658 | 1 | A1 |
| 444 | ProFTPD Detection Consolidation | 1.3.6.1.4.1.25623.1.0.155379 | 1 | A1 |
| 445 | Firebird SQL Detection Consolidation | 1.3.6.1.4.1.25623.1.0.155942 | 1 | A1 |
| 446 | PHP Detection Consolidation | 1.3.6.1.4.1.25623.1.0.171722 | 1 | A1 |
| 447 | Service Detection with 'GET' Request | 1.3.6.1.4.1.25623.1.0.17975 | 1 | A1 |
| 448 | VNC Supported 'security types' Detection (TCP) | 1.3.6.1.4.1.25623.1.0.19288 | 1 | A1 |
| 449 | 'favicon.ico' Based Fingerprinting (HTTP) | 1.3.6.1.4.1.25623.1.0.20108 | 1 | A1 |
| 450 | Traceroute | 1.3.6.1.4.1.25623.1.0.51662 | 1 | A1 |
| 451 | Firebird / InterBase Database Server Service Detection (TCP) | 1.3.6.1.4.1.25623.1.0.80004 | 1 | A1 |
| 452 | TWiki Version Detection | 1.3.6.1.4.1.25623.1.0.800399 | 1 | A1 |
| 453 | SSL/TLS: Report Supported Cipher Suites | 1.3.6.1.4.1.25623.1.0.802067 | 1 | A1 |
| 454 | Microsoft SMB Signing Disabled | 1.3.6.1.4.1.25623.1.0.802726 | 1 | A1 |
| 455 | SMB Remote Version Detection | 1.3.6.1.4.1.25623.1.0.807830 | 1 | A1 |
| 456 | CPE Inventory | 1.3.6.1.4.1.25623.1.0.810002 | 1 | A1 |
| 457 | phpMyAdmin Detection (HTTP) | 1.3.6.1.4.1.25623.1.0.900129 | 1 | A1 |

| # | Issue | Plugin ID | Hosts | Remediation |
|---|---|---|---|---|
| 458 | Microsoft Windows SMB Accessible Shares | 1.3.6.1.4.1.25623.1.0.902425 | 1 | A1 |
| 459 | SSL/TLS: Report Medium Cipher Suites | 1.3.6.1.4.1.25623.1.0.902816 | 1 | A1 |

## Methodology and data sources

What was done: the uploaded scan export was parsed; every finding passed this scan's trust-boundary checks, so none were withheld from prioritization. The remainder was enriched against a non-default KEV catalog source (not confirmed to be CISA's published catalog), ranked into priority bands, and grouped into distinct issues for this report.

Data sources: the uploaded Greenbone / OpenVAS scan export, a non-default KEV catalog source (not confirmed to be CISA's published catalog) (retrieved 2026-09-13), and a deterministic synthetic EPSS feed generated by tools/synthetic_epss_feed.py (not real EPSS data) (retrieved 2026-09-13, model score date 2026-08-30).

Band 1 (KEV + ransomware): in CISA KEV, with CISA-recorded use in known ransomware campaigns. Band 2 (KEV): in CISA KEV (CISA records these CVEs as known to have been exploited). Band 3 (urgent CVSS, no KEV match): has a CVE with no KEV match in the catalog snapshot used, and CVSS at or above the urgent threshold of 9.0. Band 4 (has CVE, non-trivial severity): has a CVE with no KEV match in the catalog snapshot used, below the urgent CVSS threshold, at a severity rating of 2 or above. Band 5 (no CVE, non-trivial severity): no CVE, but a severity rating of 2 or above. Band 6 (low or informational): any finding the bands above do not match.

Findings in this report are detections, not demonstrated exploitation. No manual penetration testing was performed. False positives and false negatives are possible, subject to the scanner's own detection limitations. This report does not, by itself, establish compliance with any regulatory or contractual framework.

This report's generation depends on a successful CISA Known Exploited Vulnerabilities catalog fetch. If the catalog cannot be retrieved and no usable cached copy exists, report generation fails rather than proceeding against an empty catalog: an empty catalog would cause every finding to render as not matching KEV, which would be a false statement about known exploitation — not a safe default.

The factors shown for each prioritized finding in this report — KEV status, EPSS exploitation-likelihood, and CVSS-derived technical severity — align descriptively with the four-variable prioritization model in CISA Binding Operational Directive 26-04 (exposure, KEV status, exploit automatability, and technical impact). This is a description of overlap only: it is not a claim that this client is subject to, or in compliance with, that directive.

# Scanner evidence appendix

Detailed vendor references and large validation inventories are kept here so the prioritized actions remain readable.

## Scanner evidence for A1

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2024-1082, CERT-BUND:WID-SEC-2023-1599, CERT-BUND:WID-SEC-2022-2413, CERT-BUND:WID-SEC-2022-1308, CERT-BUND:CB-K21/1268, DFN-CERT:DFN-CERT-2024-1260, DFN-CERT:DFN-CERT-2020-1691, CERT-BUND:WID-SEC-2024-0229, CERT-BUND:CB-K21/0979, CERT-BUND:WID-SEC-2024-3760, DFN-CERT:DFN-CERT-2022-2639, DFN-CERT:DFN-CERT-2022-2638, DFN-CERT:DFN-CERT-2022-0485, DFN-CERT:DFN-CERT-2022-0455, DFN-CERT:DFN-CERT-2022-0431, DFN-CERT:DFN-CERT-2022-0410, CERT-BUND:CB-K17/0318, CERT-BUND:CB-K16/1943, DFN-CERT:DFN-CERT-2017-0325, DFN-CERT:DFN-CERT-2016-2053, DFN-CERT:DFN-CERT-2011-0467, DFN-CERT:DFN-CERT-2011-0451, DFN-CERT:DFN-CERT-2011-0016, DFN-CERT:DFN-CERT-2011-0002 |
| Validation checks (79) | 1.3.6.1.4.1.25623.1.0.100074, 1.3.6.1.4.1.25623.1.0.100151, 1.3.6.1.4.1.25623.1.0.100152, 1.3.6.1.4.1.25623.1.0.100252, 1.3.6.1.4.1.25623.1.0.100259, 1.3.6.1.4.1.25623.1.0.10092, 1.3.6.1.4.1.25623.1.0.10107, 1.3.6.1.4.1.25623.1.0.102011, 1.3.6.1.4.1.25623.1.0.10263, 1.3.6.1.4.1.25623.1.0.10267, 1.3.6.1.4.1.25623.1.0.10281, 1.3.6.1.4.1.25623.1.0.103118, 1.3.6.1.4.1.25623.1.0.103140, 1.3.6.1.4.1.25623.1.0.103141, 1.3.6.1.4.1.25623.1.0.103210, 1.3.6.1.4.1.25623.1.0.10330, 1.3.6.1.4.1.25623.1.0.103441, 1.3.6.1.4.1.25623.1.0.103692, 1.3.6.1.4.1.25623.1.0.10394, 1.3.6.1.4.1.25623.1.0.105013, 1.3.6.1.4.1.25623.1.0.105018, 1.3.6.1.4.1.25623.1.0.105565, 1.3.6.1.4.1.25623.1.0.105782, 1.3.6.1.4.1.25623.1.0.105839, 1.3.6.1.4.1.25623.1.0.105937, 1.3.6.1.4.1.25623.1.0.108082, 1.3.6.1.4.1.25623.1.0.108090, 1.3.6.1.4.1.25623.1.0.108204, 1.3.6.1.4.1.25623.1.0.108441, 1.3.6.1.4.1.25623.1.0.108449, 1.3.6.1.4.1.25623.1.0.108478, 1.3.6.1.4.1.25623.1.0.108539, 1.3.6.1.4.1.25623.1.0.108553, 1.3.6.1.4.1.25623.1.0.108577, 1.3.6.1.4.1.25623.1.0.108708, 1.3.6.1.4.1.25623.1.0.108874, 1.3.6.1.4.1.25623.1.0.11011, 1.3.6.1.4.1.25623.1.0.111010, 1.3.6.1.4.1.25623.1.0.111038, 1.3.6.1.4.1.25623.1.0.111050, 1.3.6.1.4.1.25623.1.0.111086, 1.3.6.1.4.1.25623.1.0.11111, 1.3.6.1.4.1.25623.1.0.11156, 1.3.6.1.4.1.25623.1.0.112081, 1.3.6.1.4.1.25623.1.0.113736, 1.3.6.1.4.1.25623.1.0.113763, 1.3.6.1.4.1.25623.1.0.117232, 1.3.6.1.4.1.25623.1.0.117757, 1.3.6.1.4.1.25623.1.0.117764, 1.3.6.1.4.1.25623.1.0.117777, 1.3.6.1.4.1.25623.1.0.117799, 1.3.6.1.4.1.25623.1.0.117802, 1.3.6.1.4.1.25623.1.0.12638, 1.3.6.1.4.1.25623.1.0.128025, 1.3.6.1.4.1.25623.1.0.140151, 1.3.6.1.4.1.25623.1.0.144898, 1.3.6.1.4.1.25623.1.0.147205, 1.3.6.1.4.1.25623.1.0.150658, 1.3.6.1.4.1.25623.1.0.155379, 1.3.6.1.4.1.25623.1.0.155942, 1.3.6.1.4.1.25623.1.0.16100, 1.3.6.1.4.1.25623.1.0.171722, 1.3.6.1.4.1.25623.1.0.17975, 1.3.6.1.4.1.25623.1.0.19288, 1.3.6.1.4.1.25623.1.0.20108, 1.3.6.1.4.1.25623.1.0.51662, 1.3.6.1.4.1.25623.1.0.80004, 1.3.6.1.4.1.25623.1.0.800399, 1.3.6.1.4.1.25623.1.0.801660, 1.3.6.1.4.1.25623.1.0.802067, 1.3.6.1.4.1.25623.1.0.802726, 1.3.6.1.4.1.25623.1.0.803189, 1.3.6.1.4.1.25623.1.0.804241, 1.3.6.1.4.1.25623.1.0.807830, 1.3.6.1.4.1.25623.1.0.810002, 1.3.6.1.4.1.25623.1.0.900129, 1.3.6.1.4.1.25623.1.0.900993, 1.3.6.1.4.1.25623.1.0.902425, 1.3.6.1.4.1.25623.1.0.902816 |

## Scanner evidence for A2

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2009-1726, DFN-CERT:DFN-CERT-2010-1227, DFN-CERT:DFN-CERT-2010-0265, DFN-CERT:DFN-CERT-2010-0263, DFN-CERT:DFN-CERT-2010-0253, DFN-CERT:DFN-CERT-2010-0143, DFN-CERT:DFN-CERT-2010-0140, DFN-CERT:DFN-CERT-2010-0075, DFN-CERT:DFN-CERT-2010-0074, DFN-CERT:DFN-CERT-2010-0073, DFN-CERT:DFN-CERT-2010-0060, DFN-CERT:DFN-CERT-2010-1620, DFN-CERT:DFN- |

| | |
|---|---|
| | CERT-2010-0997, DFN-CERT:DFN-CERT-2010-0906, DFN-CERT:DFN-CERT-2010-0802, DFN-CERT:DFN-CERT-2009-1652, DFN-CERT:DFN-CERT-2009-1508, DFN-CERT:DFN-CERT-2009-1340, DFN-CERT:DFN-CERT-2011-1005, DFN-CERT:DFN-CERT-2011-0642, DFN-CERT:DFN-CERT-2010-1321, DFN-CERT:DFN-CERT-2010-1247, DFN-CERT:DFN-CERT-2010-1079, DFN-CERT:DFN-CERT-2010-0953, DFN-CERT:DFN-CERT-2010-0775, DFN-CERT:DFN-CERT-2010-0705, DFN-CERT:DFN-CERT-2010-0419, DFN-CERT:DFN-CERT-2010-0372, DFN-CERT:DFN-CERT-2009-1418, DFN-CERT:DFN-CERT-2009-1497, DFN-CERT:DFN-CERT-2010-0588, DFN-CERT:DFN-CERT-2011-0515, CERT-BUND:CB-K14/1413, DFN-CERT:DFN-CERT-2014-1494, DFN-CERT:DFN-CERT-2011-0148, DFN-CERT:DFN-CERT-2009-1639, DFN-CERT:DFN-CERT-2009-1490, DFN-CERT:DFN-CERT-2009-1487, DFN-CERT:DFN-CERT-2009-1376, DFN-CERT:DFN-CERT-2009-1375, DFN-CERT:DFN-CERT-2009-1374 |
| Validation checks (17) | 1.3.6.1.4.1.25623.1.0.100146, 1.3.6.1.4.1.25623.1.0.100409, 1.3.6.1.4.1.25623.1.0.100511, 1.3.6.1.4.1.25623.1.0.100581, 1.3.6.1.4.1.25623.1.0.108861, 1.3.6.1.4.1.25623.1.0.108866, 1.3.6.1.4.1.25623.1.0.108867, 1.3.6.1.4.1.25623.1.0.108868, 1.3.6.1.4.1.25623.1.0.800110, 1.3.6.1.4.1.25623.1.0.800334, 1.3.6.1.4.1.25623.1.0.801731, 1.3.6.1.4.1.25623.1.0.805410, 1.3.6.1.4.1.25623.1.0.900184, 1.3.6.1.4.1.25623.1.0.900185, 1.3.6.1.4.1.25623.1.0.900186, 1.3.6.1.4.1.25623.1.0.900871, 1.3.6.1.4.1.25623.1.0.900925 |

## Scanner evidence for A3

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2024-1226, CERT-BUND:WID-SEC-2024-0899, CERT-BUND:WID-SEC-2024-0869, CERT-BUND:WID-SEC-2024-0769, CERT-BUND:WID-SEC-2024-0107, CERT-BUND:WID-SEC-2023-2917, CERT-BUND:WID-SEC-2023-2712, DFN-CERT:DFN-CERT-2026-2996, DFN-CERT:DFN-CERT-2024-1411, DFN-CERT:DFN-CERT-2024-1010, DFN-CERT:DFN-CERT-2024-1000, DFN-CERT:DFN-CERT-2024-0732, DFN-CERT:DFN-CERT-2023-2640, DFN-CERT:DFN-CERT-2023-2583, CERT-BUND:WID-SEC-2024-1591, CERT-BUND:WID-SEC-2022-1772, CERT-BUND:WID-SEC-2022-1335, CERT-BUND:WID-SEC-2022-1228, CERT-BUND:WID-SEC-2022-1161, CERT-BUND:WID-SEC-2022-1057, CERT-BUND:WID-SEC-2022-0898, CERT-BUND:WID-SEC-2022-0799, CERT-BUND:WID-SEC-2022-0755, CERT-BUND:WID-SEC-2022-0646, CERT-BUND:WID-SEC-2022-0432, CERT-BUND:WID-SEC-2022-0302, CERT-BUND:WID-SEC-2022-0290, CERT-BUND:CB-K22/0619, CERT-BUND:CB-K22/0306, DFN-CERT:DFN-CERT-2022-2799, DFN-CERT:DFN-CERT-2022-2509, DFN-CERT:DFN-CERT-2022-2305, DFN-CERT:DFN-CERT-2022-2167, DFN-CERT:DFN-CERT-2022-1116, DFN-CERT:DFN-CERT-2022-1115, DFN-CERT:DFN-CERT-2022-1114, DFN-CERT:DFN-CERT-2022-0899, DFN-CERT:DFN-CERT-2022-0898, DFN-CERT:DFN-CERT-2022-0865, DFN-CERT:DFN-CERT-2022-0747, DFN-CERT:DFN-CERT-2022-0678, DFN-CERT:DFN-CERT-2022-0582, CERT-BUND:WID-SEC-2025-1572, CERT-BUND:WID-SEC-2025-0818, CERT-BUND:WID-SEC-2025-0148, CERT-BUND:WID-SEC-2025-0143, CERT-BUND:WID-SEC-2024-3291, CERT-BUND:WID-SEC-2024-3199, CERT-BUND:WID-SEC-2024-1913, CERT-BUND:WID-SEC-2024-1504, DFN-CERT:DFN-CERT-2026-2301, DFN-CERT:DFN-CERT-2025-1898, DFN-CERT:DFN-CERT-2025-1808, DFN-CERT:DFN-CERT-2025-0974, DFN-CERT:DFN-CERT-2025-0854, DFN-CERT:DFN-CERT-2025-0170, DFN-CERT:DFN-CERT-2024-2841, DFN-CERT:DFN-CERT-2024-2787, DFN-CERT:DFN-CERT-2024-2736, DFN-CERT:DFN-CERT-2024-2342, DFN-CERT:DFN-CERT-2024-2214, DFN-CERT:DFN-CERT-2024-2201, DFN-CERT:DFN-CERT-2024-2180, DFN-CERT:DFN-CERT-2024-2110, DFN-CERT:DFN-CERT-2024-2017, DFN-CERT:DFN-CERT-2024-1963, DFN-CERT:DFN-CERT-2024-1920, DFN-CERT:DFN-CERT-2024-1919, DFN-CERT:DFN-CERT-2024-1911, DFN-CERT:DFN-CERT-2024-1907, DFN-CERT:DFN-CERT-2024-1893, DFN-CERT:DFN-CERT-2024-1816, DFN-CERT:DFN-CERT-2024-1811, DFN-CERT:DFN-CERT-2024-1784, DFN-CERT:DFN-CERT-2024-1741, DFN-CERT:DFN-CERT-2024-1699, CERT-BUND:WID-SEC-2024-0064, CERT-BUND:WID-SEC-2022-1908, CERT-BUND:WID-SEC-2022-1767, CERT-BUND:WID-SEC-2022-0727, CERT-BUND:WID-SEC-2022-0190, CERT-BUND:CB-K21/1296, DFN-CERT:DFN-CERT-2022-0369, DFN-CERT:DFN-CERT-2022-0192, DFN-CERT:DFN-CERT-2022-0098, DFN-CERT:DFN-CERT-2022-0068, DFN-CERT:DFN-CERT-2021-2656, CERT-BUND:WID-SEC-2026-2189, CERT-BUND:WID-SEC-2026-1730, CERT- |

BUND:WID-SEC-2026-1203, CERT-BUND:WID-SEC-2026-1194, CERT-BUND:WID-SEC-2026-0853, CERT-BUND:WID-SEC-2026-0349, CERT-BUND:WID-SEC-2026-0153, CERT-BUND:WID-SEC-2025-2750, DFN-CERT:DFN-CERT-2026-2380, DFN-CERT:DFN-CERT-2026-1581, DFN-CERT:DFN-CERT-2026-1112, DFN-CERT:DFN-CERT-2026-1111, DFN-CERT:DFN-CERT-2026-1110, DFN-CERT:DFN-CERT-2026-0680, DFN-CERT:DFN-CERT-2026-0027, DFN-CERT:DFN-CERT-2026-0012, DFN-CERT:DFN-CERT-2025-3602, DFN-CERT:DFN-CERT-2025-3581, DFN-CERT:DFN-CERT-2025-3512, DFN-CERT:DFN-CERT-2025-3405, CERT-BUND:WID-SEC-2024-2180, CERT-BUND:WID-SEC-2024-0186, CERT-BUND:WID-SEC-2023-1969, CERT-BUND:WID-SEC-2023-1016, CERT-BUND:WID-SEC-2022-1298, CERT-BUND:WID-SEC-2022-1189, CERT-BUND:WID-SEC-2022-0724, CERT-BUND:CB-K22/0476, CERT-BUND:CB-K22/0465, CERT-BUND:CB-K22/0463, CERT-BUND:CB-K21/0992, DFN-CERT:DFN-CERT-2023-0881, DFN-CERT:DFN-CERT-2022-2405, DFN-CERT:DFN-CERT-2022-0904, DFN-CERT:DFN-CERT-2022-0878, DFN-CERT:DFN-CERT-2022-0872, DFN-CERT:DFN-CERT-2022-0869, DFN-CERT:DFN-CERT-2022-0672, DFN-CERT:DFN-CERT-2022-0207, DFN-CERT:DFN-CERT-2022-0119, DFN-CERT:DFN-CERT-2021-2629, DFN-CERT:DFN-CERT-2021-2471, DFN-CERT:DFN-CERT-2021-2185, DFN-CERT:DFN-CERT-2021-2164, DFN-CERT:DFN-CERT-2021-2153, DFN-CERT:DFN-CERT-2021-2098, DFN-CERT:DFN-CERT-2021-2090, DFN-CERT:DFN-CERT-2021-2047, DFN-CERT:DFN-CERT-2021-2020, DFN-CERT:DFN-CERT-2021-1961, CERT-BUND:WID-SEC-2023-0134, CERT-BUND:WID-SEC-2023-0132, CERT-BUND:WID-SEC-2022-1766, CERT-BUND:WID-SEC-2022-1764, CERT-BUND:WID-SEC-2022-0858, CERT-BUND:WID-SEC-2022-0192, CERT-BUND:CB-K22/0692, DFN-CERT:DFN-CERT-2023-0119, DFN-CERT:DFN-CERT-2022-2789, DFN-CERT:DFN-CERT-2022-2652, DFN-CERT:DFN-CERT-2022-2310, DFN-CERT:DFN-CERT-2022-1837, DFN-CERT:DFN-CERT-2022-1833, DFN-CERT:DFN-CERT-2022-1720, DFN-CERT:DFN-CERT-2022-1353, DFN-CERT:DFN-CERT-2022-1296, CERT-BUND:WID-SEC-2024-3195, CERT-BUND:WID-SEC-2024-0794, CERT-BUND:WID-SEC-2023-2674, CERT-BUND:WID-SEC-2023-1424, CERT-BUND:WID-SEC-2023-1022, CERT-BUND:WID-SEC-2023-0561, CERT-BUND:WID-SEC-2023-0110, DFN-CERT:DFN-CERT-2023-2545, DFN-CERT:DFN-CERT-2023-1895, DFN-CERT:DFN-CERT-2023-1297, DFN-CERT:DFN-CERT-2023-0658, DFN-CERT:DFN-CERT-2023-0548, DFN-CERT:DFN-CERT-2023-0497, DFN-CERT:DFN-CERT-2023-0118, CERT-BUND:WID-SEC-2025-1529, CERT-BUND:WID-SEC-2024-1725, CERT-BUND:WID-SEC-2024-1643, CERT-BUND:WID-SEC-2024-1642, CERT-BUND:WID-SEC-2024-1248, CERT-BUND:WID-SEC-2024-0801, CERT-BUND:WID-SEC-2024-0789, DFN-CERT:DFN-CERT-2026-4515, DFN-CERT:DFN-CERT-2026-3742, DFN-CERT:DFN-CERT-2026-3594, DFN-CERT:DFN-CERT-2025-2802, DFN-CERT:DFN-CERT-2025-2658, DFN-CERT:DFN-CERT-2025-2657, DFN-CERT:DFN-CERT-2024-2900, DFN-CERT:DFN-CERT-2024-2534, DFN-CERT:DFN-CERT-2024-2076, DFN-CERT:DFN-CERT-2024-1958, DFN-CERT:DFN-CERT-2024-1853, DFN-CERT:DFN-CERT-2024-1749, DFN-CERT:DFN-CERT-2024-1697, DFN-CERT:DFN-CERT-2024-1335, DFN-CERT:DFN-CERT-2024-1238, DFN-CERT:DFN-CERT-2024-1031, DFN-CERT:DFN-CERT-2024-0964, DFN-CERT:DFN-CERT-2024-0901, DFN-CERT:DFN-CERT-2024-0890, CERT-BUND:WID-SEC-2026-0162, CERT-BUND:WID-SEC-2025-1850, DFN-CERT:DFN-CERT-2026-3672, DFN-CERT:DFN-CERT-2026-3546, DFN-CERT:DFN-CERT-2026-3044, DFN-CERT:DFN-CERT-2026-2662, DFN-CERT:DFN-CERT-2026-0205, DFN-CERT:DFN-CERT-2025-2421, DFN-CERT:DFN-CERT-2025-2403, DFN-CERT:DFN-CERT-2025-2402, DFN-CERT:DFN-CERT-2025-2373, DFN-CERT:DFN-CERT-2025-2231, DFN-CERT:DFN-CERT-2025-2182, DFN-CERT:DFN-CERT-2025-1917, DFN-CERT:DFN-CERT-2025-1860

## Scanner evidence for A4

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2011-1005, DFN-CERT:DFN-CERT-2011-0642, DFN-CERT:DFN-CERT-2010-1620, DFN-CERT:DFN-CERT-2010-1321, DFN-CERT:DFN-CERT-2010-1247, DFN-CERT:DFN-CERT-2010-1079, DFN-CERT:DFN-CERT-2010-0997, DFN-CERT:DFN-CERT-2010-0953, DFN-CERT:DFN-CERT-2011-0402, DFN-CERT:DFN-CERT-2011-0148, DFN-CERT:DFN-CERT-2010-1664, DFN-CERT:DFN-CERT-2010-1530, DFN-CERT:DFN- |

CERT-2011-0520, DFN-CERT:DFN-CERT-2011-0518, DFN-CERT:DFN-CERT-2011-0517, DFN-CERT:DFN-CERT-2011-0445, DFN-CERT:DFN-CERT-2011-0444, DFN-CERT:DFN-CERT-2011-0442, DFN-CERT:DFN-CERT-2011-0441, DFN-CERT:DFN-CERT-2011-0432, CERT-BUND:CB-K15/1514, CERT-BUND:CB-K13/0921, DFN-CERT:DFN-CERT-2013-1938, DFN-CERT:DFN-CERT-2013-1494, DFN-CERT:DFN-CERT-2012-0914, DFN-CERT:DFN-CERT-2012-0731, DFN-CERT:DFN-CERT-2012-0714, DFN-CERT:DFN-CERT-2012-0678, DFN-CERT:DFN-CERT-2012-0172, DFN-CERT:DFN-CERT-2012-0167, DFN-CERT:DFN-CERT-2012-0165, DFN-CERT:DFN-CERT-2012-0099, DFN-CERT:DFN-CERT-2011-1816, DFN-CERT:DFN-CERT-2011-1814, DFN-CERT:DFN-CERT-2011-1813, DFN-CERT:DFN-CERT-2011-1708, DFN-CERT:DFN-CERT-2011-1698, DFN-CERT:DFN-CERT-2011-1686, DFN-CERT:DFN-CERT-2011-1643, DFN-CERT:DFN-CERT-2011-1603, DFN-CERT:DFN-CERT-2011-1602, DFN-CERT:DFN-CERT-2011-1443, DFN-CERT:DFN-CERT-2011-1433, DFN-CERT:DFN-CERT-2011-1402, DFN-CERT:DFN-CERT-2011-1396, DFN-CERT:DFN-CERT-2011-1387, DFN-CERT:DFN-CERT-2011-1276, DFN-CERT:DFN-CERT-2012-1276, DFN-CERT:DFN-CERT-2012-1268, DFN-CERT:DFN-CERT-2012-1267, DFN-CERT:DFN-CERT-2012-1266, DFN-CERT:DFN-CERT-2012-0641, DFN-CERT:DFN-CERT-2012-0586, DFN-CERT:DFN-CERT-2012-0538, DFN-CERT:DFN-CERT-2010-0775, DFN-CERT:DFN-CERT-2010-0705, DFN-CERT:DFN-CERT-2010-0419, DFN-CERT:DFN-CERT-2010-0372, CERT-BUND:CB-K16/0944, CERT-BUND:CB-K15/0703, CERT-BUND:CB-K14/0323, CERT-BUND:CB-K13/0712, DFN-CERT:DFN-CERT-2016-1004, DFN-CERT:DFN-CERT-2015-0732, DFN-CERT:DFN-CERT-2014-0336, DFN-CERT:DFN-CERT-2013-1713, DFN-CERT:DFN-CERT-2012-0210, DFN-CERT:DFN-CERT-2012-0109, DFN-CERT:DFN-CERT-2011-0515, DFN-CERT:DFN-CERT-2011-0147, DFN-CERT:DFN-CERT-2011-0036, DFN-CERT:DFN-CERT-2011-0013, DFN-CERT:DFN-CERT-2011-0012, DFN-CERT:DFN-CERT-2011-0011, DFN-CERT:DFN-CERT-2010-1729, DFN-CERT:DFN-CERT-2010-1706, DFN-CERT:DFN-CERT-2010-1593, DFN-CERT:DFN-CERT-2010-1526, DFN-CERT:DFN-CERT-2010-1471

## Scanner evidence for A5

The action above covers the following detailed scanner evidence.

Vendor references

CERT-BUND:CB-K17/1252, CERT-BUND:CB-K16/1776, CERT-BUND:CB-K16/0975, CERT-BUND:CB-K16/0965, CERT-BUND:CB-K16/0944, CERT-BUND:CB-K16/0937, CERT-BUND:CB-K16/0912, CERT-BUND:CB-K16/0911, CERT-BUND:CB-K16/0868, CERT-BUND:CB-K16/0805, CERT-BUND:CB-K16/0801, DFN-CERT:DFN-CERT-2017-1295, DFN-CERT:DFN-CERT-2016-1882, DFN-CERT:DFN-CERT-2016-1033, DFN-CERT:DFN-CERT-2016-1022, DFN-CERT:DFN-CERT-2016-1004, DFN-CERT:DFN-CERT-2016-0996, DFN-CERT:DFN-CERT-2016-0972, DFN-CERT:DFN-CERT-2016-0944, DFN-CERT:DFN-CERT-2016-0924, DFN-CERT:DFN-CERT-2016-0876, DFN-CERT:DFN-CERT-2016-0871, DFN-CERT:DFN-CERT-2016-0857, DFN-CERT:DFN-CERT-2016-0855, CERT-BUND:CB-K15/1158, CERT-BUND:CB-K15/1031, CERT-BUND:CB-K15/0966, CERT-BUND:CB-K15/0942, CERT-BUND:CB-K15/0936, CERT-BUND:CB-K15/0854, DFN-CERT:DFN-CERT-2015-1217, DFN-CERT:DFN-CERT-2015-1083, DFN-CERT:DFN-CERT-2015-1017, DFN-CERT:DFN-CERT-2015-0989, DFN-CERT:DFN-CERT-2015-0983, DFN-CERT:DFN-CERT-2015-0900, CERT-BUND:CB-K16/1958, CERT-BUND:CB-K16/1543, CERT-BUND:CB-K16/1532, CERT-BUND:CB-K16/1426, DFN-CERT:DFN-CERT-2016-2063, DFN-CERT:DFN-CERT-2016-1639, DFN-CERT:DFN-CERT-2016-1631, DFN-CERT:DFN-CERT-2016-1495, CERT-BUND:CB-K18/0048, CERT-BUND:CB-K17/1461, CERT-BUND:CB-K17/1358, CERT-BUND:CB-K17/1132, DFN-CERT:DFN-CERT-2018-0835, DFN-CERT:DFN-CERT-2018-0733, DFN-CERT:DFN-CERT-2018-0055, DFN-CERT:DFN-CERT-2017-1529, DFN-CERT:DFN-CERT-2017-1420, DFN-CERT:DFN-CERT-2017-1161

## Scanner evidence for A6

The action above covers the following detailed scanner evidence.

Vendor references

CERT-BUND:WID-SEC-2022-2122, CERT-BUND:CB-K20/1199, CERT-BUND:CB-K19/1099, DFN-CERT:DFN-CERT-2022-2638, DFN-CERT:DFN-CERT-2020-2627, DFN-CERT:DFN-CERT-2020-1964, DFN-CERT:DFN-CERT-2020-0415, DFN-CERT:DFN-CERT-2020-0382, DFN-

CERT:DFN-CERT-2020-0339, DFN-CERT:DFN-CERT-2019-2709, DFN-CERT:DFN-CERT-2019-2659, CERT-BUND:WID-SEC-2022-2119, CERT-BUND:CB-K20/0147, DFN-CERT:DFN-CERT-2020-1438, DFN-CERT:DFN-CERT-2020-0787, DFN-CERT:DFN-CERT-2020-0518, DFN-CERT:DFN-CERT-2020-0485, DFN-CERT:DFN-CERT-2020-0341, CERT-BUND:WID-SEC-2022-2118, CERT-BUND:CB-K21/0068, CERT-BUND:CB-K20/0239, DFN-CERT:DFN-CERT-2020-1202, DFN-CERT:DFN-CERT-2020-0965, DFN-CERT:DFN-CERT-2020-0851, DFN-CERT:DFN-CERT-2020-0554

## Scanner evidence for A7

The action above covers the following detailed scanner evidence.

Vendor references: CERT-BUND:CB-K19/0477, DFN-CERT:DFN-CERT-2019-1217, DFN-CERT:DFN-CERT-2019-1127, CERT-BUND:CB-K19/0836, DFN-CERT:DFN-CERT-2020-0089, DFN-CERT:DFN-CERT-2019-1975, CERT-BUND:CB-K20/0214, CERT-BUND:CB-K19/1043, CERT-BUND:CB-K19/1016, DFN-CERT:DFN-CERT-2020-2322, DFN-CERT:DFN-CERT-2020-0488, DFN-CERT:DFN-CERT-2019-2577, DFN-CERT:DFN-CERT-2019-2465

## Scanner evidence for A8

The action above covers the following detailed scanner evidence.

Vendor references: DFN-CERT:DFN-CERT-2011-0368, DFN-CERT:DFN-CERT-2009-1344

## Scanner evidence for A9

The action above covers the following detailed scanner evidence.

Vendor references: CERT-BUND:CB-K17/0896, CERT-BUND:CB-K17/0517, CERT-BUND:CB-K14/0825, DFN-CERT:DFN-CERT-2020-0232, DFN-CERT:DFN-CERT-2017-0925, DFN-CERT:DFN-CERT-2017-0534, DFN-CERT:DFN-CERT-2016-0890, DFN-CERT:DFN-CERT-2014-0863, DFN-CERT:DFN-CERT-2012-0424, DFN-CERT:DFN-CERT-2012-0387, DFN-CERT:DFN-CERT-2012-0306, DFN-CERT:DFN-CERT-2011-0700, DFN-CERT:DFN-CERT-2010-1647, DFN-CERT:DFN-CERT-2010-1271, DFN-CERT:DFN-CERT-2010-0730, DFN-CERT:DFN-CERT-2010-0725, DFN-CERT:DFN-CERT-2010-0619, DFN-CERT:DFN-CERT-2010-0599, DFN-CERT:DFN-CERT-2010-0586, DFN-CERT:DFN-CERT-2010-0567, DFN-CERT:DFN-CERT-2010-0414, DFN-CERT:DFN-CERT-2010-0402, DFN-CERT:DFN-CERT-2010-0314, DFN-CERT:DFN-CERT-2010-0290, CERT-BUND:CB-K15/1073, CERT-BUND:CB-K15/0080, CERT-BUND:CB-K15/0079, CERT-BUND:CB-K14/1505, CERT-BUND:CB-K14/0608, DFN-CERT:DFN-CERT-2015-1135, DFN-CERT:DFN-CERT-2015-0082, DFN-CERT:DFN-CERT-2015-0079, DFN-CERT:DFN-CERT-2014-1592, DFN-CERT:DFN-CERT-2014-0635, DFN-CERT:DFN-CERT-2013-1307, DFN-CERT:DFN-CERT-2012-1276, DFN-CERT:DFN-CERT-2012-1112, DFN-CERT:DFN-CERT-2012-0928, DFN-CERT:DFN-CERT-2012-0771, DFN-CERT:DFN-CERT-2012-0758, DFN-CERT:DFN-CERT-2012-0744, DFN-CERT:DFN-CERT-2012-0740, DFN-CERT:DFN-CERT-2012-0568, DFN-CERT:DFN-CERT-2012-0425, DFN-CERT:DFN-CERT-2012-0343, DFN-CERT:DFN-CERT-2012-0332, DFN-CERT:DFN-CERT-2012-0264, DFN-CERT:DFN-CERT-2012-0228, DFN-CERT:DFN-CERT-2012-0203, DFN-CERT:DFN-CERT-2012-0188, DFN-CERT:DFN-CERT-2012-0048

## Scanner evidence for A10

The action above covers the following detailed scanner evidence.

Vendor references: CERT-BUND:WID-SEC-2026-1752, CERT-BUND:WID-SEC-2022-0673, CERT-BUND:CB-K22/0045, CERT-BUND:CB-K18/1131, DFN-CERT:DFN-CERT-2025-1803, DFN-CERT:DFN-CERT-2023-1197, DFN-CERT:DFN-CERT-2020-0590, CERT-BUND:WID-SEC-2023-0558, CERT-BUND:WID-

SEC-2022-0736, DFN-CERT:DFN-CERT-2022-1614, DFN-CERT:DFN-CERT-2021-2348, DFN-CERT:DFN-CERT-2021-1503, DFN-CERT:DFN-CERT-2020-2259, DFN-CERT:DFN-CERT-2020-2209

## Scanner evidence for A11

The action above covers the following detailed scanner evidence.

Vendor references

CERT-BUND:WID-SEC-2025-1087, CERT-BUND:WID-SEC-2024-3217, CERT-BUND:WID-SEC-2024-1872, CERT-BUND:WID-SEC-2023-0239, CERT-BUND:WID-SEC-2023-0063, CERT-BUND:WID-SEC-2022-1767, CERT-BUND:WID-SEC-2022-1347, CERT-BUND:WID-SEC-2022-0740, CERT-BUND:WID-SEC-2022-0732, CERT-BUND:WID-SEC-2022-0624, CERT-BUND:CB-K22/0463, CERT-BUND:CB-K21/1085, CERT-BUND:CB-K21/0071, CERT-BUND:CB-K21/0070, CERT-BUND:CB-K21/0069, CERT-BUND:CB-K21/0067, CERT-BUND:CB-K21/0061, CERT-BUND:CB-K21/0059, CERT-BUND:CB-K20/1049, CERT-BUND:CB-K20/1030, CERT-BUND:CB-K20/1027, CERT-BUND:CB-K20/1025, CERT-BUND:CB-K20/1023, CERT-BUND:CB-K20/1008, CERT-BUND:CB-K20/0870, CERT-BUND:CB-K20/0800, CERT-BUND:CB-K20/0705, CERT-BUND:CB-K20/0521, DFN-CERT:DFN-CERT-2025-1803, DFN-CERT:DFN-CERT-2025-0559, DFN-CERT:DFN-CERT-2025-0041, DFN-CERT:DFN-CERT-2023-2027, DFN-CERT:DFN-CERT-2023-1197, DFN-CERT:DFN-CERT-2023-0481, DFN-CERT:DFN-CERT-2023-0245, DFN-CERT:DFN-CERT-2022-1988, DFN-CERT:DFN-CERT-2022-1670, DFN-CERT:DFN-CERT-2022-0869, DFN-CERT:DFN-CERT-2022-0074, DFN-CERT:DFN-CERT-2021-2190, DFN-CERT:DFN-CERT-2021-1111, DFN-CERT:DFN-CERT-2021-0828, DFN-CERT:DFN-CERT-2021-0826, DFN-CERT:DFN-CERT-2021-0819, DFN-CERT:DFN-CERT-2021-0633, DFN-CERT:DFN-CERT-2021-0545, DFN-CERT:DFN-CERT-2021-0140, DFN-CERT:DFN-CERT-2021-0138, DFN-CERT:DFN-CERT-2021-0135, DFN-CERT:DFN-CERT-2021-0132, DFN-CERT:DFN-CERT-2020-2423, DFN-CERT:DFN-CERT-2020-2335, DFN-CERT:DFN-CERT-2020-2305, DFN-CERT:DFN-CERT-2020-2286, DFN-CERT:DFN-CERT-2020-2227, DFN-CERT:DFN-CERT-2020-2209, DFN-CERT:DFN-CERT-2020-2130, DFN-CERT:DFN-CERT-2020-2074, DFN-CERT:DFN-CERT-2020-2015, DFN-CERT:DFN-CERT-2020-2001, DFN-CERT:DFN-CERT-2020-1838, DFN-CERT:DFN-CERT-2020-1812, DFN-CERT:DFN-CERT-2020-1712, DFN-CERT:DFN-CERT-2020-1509, DFN-CERT:DFN-CERT-2020-1506, DFN-CERT:DFN-CERT-2020-1433, DFN-CERT:DFN-CERT-2020-1163, DFN-CERT:DFN-CERT-2020-1161, DFN-CERT:DFN-CERT-2020-1138, DFN-CERT:DFN-CERT-2020-1099, CERT-BUND:WID-SEC-2025-1459, CERT-BUND:WID-SEC-2024-3191, CERT-BUND:WID-SEC-2022-1189, CERT-BUND:WID-SEC-2022-0757, CERT-BUND:CB-K21/1067, CERT-BUND:CB-K21/0418, CERT-BUND:CB-K20/1024, CERT-BUND:CB-K20/1021, DFN-CERT:DFN-CERT-2025-2802, DFN-CERT:DFN-CERT-2025-0497, DFN-CERT:DFN-CERT-2025-0373, DFN-CERT:DFN-CERT-2025-0348, DFN-CERT:DFN-CERT-2024-2743, DFN-CERT:DFN-CERT-2022-1610, DFN-CERT:DFN-CERT-2022-0119, DFN-CERT:DFN-CERT-2021-2348, DFN-CERT:DFN-CERT-2021-1687, DFN-CERT:DFN-CERT-2021-0820, DFN-CERT:DFN-CERT-2021-0563, DFN-CERT:DFN-CERT-2020-2776, DFN-CERT:DFN-CERT-2020-2287, DFN-CERT:DFN-CERT-2020-1743

## Scanner evidence for A15

The action above covers the following detailed scanner evidence.

Vendor references

CERT-BUND:WID-SEC-2026-0180, CERT-BUND:CB-K21/0067, CERT-BUND:CB-K19/0812, CERT-BUND:CB-K17/1750, CERT-BUND:CB-K16/1593, CERT-BUND:CB-K16/1552, CERT-BUND:CB-K16/1102, CERT-BUND:CB-K16/0617, CERT-BUND:CB-K16/0599, CERT-BUND:CB-K16/0168, CERT-BUND:CB-K16/0121, CERT-BUND:CB-K16/0090, CERT-BUND:CB-K16/0030, CERT-BUND:CB-K15/1751, CERT-BUND:CB-K15/1591, CERT-BUND:CB-K15/1550, CERT-BUND:CB-K15/1517, CERT-BUND:CB-K15/1514, CERT-BUND:CB-K15/1464, CERT-BUND:CB-K15/1442, CERT-BUND:CB-K15/1334, CERT-BUND:CB-K15/1269, CERT-BUND:CB-K15/1136, CERT-BUND:CB-K15/1090, CERT-BUND:CB-K15/1059, CERT-BUND:CB-K15/1022, CERT-BUND:CB-K15/1015, CERT-BUND:CB-K15/0986, CERT-BUND:CB-K15/0964, CERT-BUND:CB-K15/0962, CERT-BUND:CB-K15/0932, CERT-BUND:CB-K15/0927, CERT-BUND:CB-K15/0926, CERT-BUND:CB-K15/0907, CERT-BUND:CB-K15/0901, CERT-BUND:CB-K15/0896, CERT-BUND:CB-

K15/0889, CERT-BUND:CB-K15/0877, CERT-BUND:CB-K15/0850, CERT-BUND:CB-K15/0849, CERT-BUND:CB-K15/0834, CERT-BUND:CB-K15/0827, CERT-BUND:CB-K15/0802, CERT-BUND:CB-K15/0764, CERT-BUND:CB-K15/0733, CERT-BUND:CB-K15/0667, CERT-BUND:CB-K14/0935, CERT-BUND:CB-K13/0942, DFN-CERT:DFN-CERT-2023-2939, DFN-CERT:DFN-CERT-2021-0775, DFN-CERT:DFN-CERT-2020-1561, DFN-CERT:DFN-CERT-2020-1276, DFN-CERT:DFN-CERT-2017-1821, DFN-CERT:DFN-CERT-2016-1692, DFN-CERT:DFN-CERT-2016-1648, DFN-CERT:DFN-CERT-2016-1168, DFN-CERT:DFN-CERT-2016-0665, DFN-CERT:DFN-CERT-2016-0642, DFN-CERT:DFN-CERT-2016-0184, DFN-CERT:DFN-CERT-2016-0135, DFN-CERT:DFN-CERT-2016-0101, DFN-CERT:DFN-CERT-2016-0035, DFN-CERT:DFN-CERT-2015-1853, DFN-CERT:DFN-CERT-2015-1679, DFN-CERT:DFN-CERT-2015-1632, DFN-CERT:DFN-CERT-2015-1608, DFN-CERT:DFN-CERT-2015-1542, DFN-CERT:DFN-CERT-2015-1518, DFN-CERT:DFN-CERT-2015-1406, DFN-CERT:DFN-CERT-2015-1341, DFN-CERT:DFN-CERT-2015-1194, DFN-CERT:DFN-CERT-2015-1144, DFN-CERT:DFN-CERT-2015-1113, DFN-CERT:DFN-CERT-2015-1078, DFN-CERT:DFN-CERT-2015-1067, DFN-CERT:DFN-CERT-2015-1038, DFN-CERT:DFN-CERT-2015-1016, DFN-CERT:DFN-CERT-2015-1012, DFN-CERT:DFN-CERT-2015-0980, DFN-CERT:DFN-CERT-2015-0977, DFN-CERT:DFN-CERT-2015-0976, DFN-CERT:DFN-CERT-2015-0960, DFN-CERT:DFN-CERT-2015-0956, DFN-CERT:DFN-CERT-2015-0944, DFN-CERT:DFN-CERT-2015-0937, DFN-CERT:DFN-CERT-2015-0925, DFN-CERT:DFN-CERT-2015-0884, DFN-CERT:DFN-CERT-2015-0881, DFN-CERT:DFN-CERT-2015-0879, DFN-CERT:DFN-CERT-2015-0866, DFN-CERT:DFN-CERT-2015-0844, DFN-CERT:DFN-CERT-2015-0800, DFN-CERT:DFN-CERT-2015-0737, DFN-CERT:DFN-CERT-2015-0696, DFN-CERT:DFN-CERT-2014-0977

## Scanner evidence for A18

The action above covers the following detailed scanner evidence.

Vendor references

CERT-BUND:WID-SEC-2026-0180, CERT-BUND:WID-SEC-2025-1658, CERT-BUND:WID-SEC-2023-0431, CERT-BUND:WID-SEC-2023-0427, CERT-BUND:CB-K18/0094, CERT-BUND:CB-K17/1198, CERT-BUND:CB-K17/1196, CERT-BUND:CB-K16/1828, CERT-BUND:CB-K16/1438, CERT-BUND:CB-K16/1384, CERT-BUND:CB-K16/1141, CERT-BUND:CB-K16/1107, CERT-BUND:CB-K16/1102, CERT-BUND:CB-K16/0792, CERT-BUND:CB-K16/0599, CERT-BUND:CB-K16/0597, CERT-BUND:CB-K16/0459, CERT-BUND:CB-K16/0456, CERT-BUND:CB-K16/0433, CERT-BUND:CB-K16/0424, CERT-BUND:CB-K16/0415, CERT-BUND:CB-K16/0413, CERT-BUND:CB-K16/0374, CERT-BUND:CB-K16/0367, CERT-BUND:CB-K16/0331, CERT-BUND:CB-K16/0329, CERT-BUND:CB-K16/0328, CERT-BUND:CB-K16/0156, CERT-BUND:CB-K15/1514, CERT-BUND:CB-K15/1358, CERT-BUND:CB-K15/1021, CERT-BUND:CB-K15/0972, CERT-BUND:CB-K15/0637, CERT-BUND:CB-K15/0590, CERT-BUND:CB-K15/0525, CERT-BUND:CB-K15/0393, CERT-BUND:CB-K15/0384, CERT-BUND:CB-K15/0287, CERT-BUND:CB-K15/0252, CERT-BUND:CB-K15/0246, CERT-BUND:CB-K15/0237, CERT-BUND:CB-K15/0118, CERT-BUND:CB-K15/0110, CERT-BUND:CB-K15/0108, CERT-BUND:CB-K15/0080, CERT-BUND:CB-K15/0078, CERT-BUND:CB-K15/0077, CERT-BUND:CB-K15/0075, CERT-BUND:CB-K14/1617, CERT-BUND:CB-K14/1581, CERT-BUND:CB-K14/1537, CERT-BUND:CB-K14/1479, CERT-BUND:CB-K14/1458, CERT-BUND:CB-K14/1342, CERT-BUND:CB-K14/1314, CERT-BUND:CB-K14/1313, CERT-BUND:CB-K14/1311, CERT-BUND:CB-K14/1304, CERT-BUND:CB-K14/1296, DFN-CERT:DFN-CERT-2018-0096, DFN-CERT:DFN-CERT-2017-1238, DFN-CERT:DFN-CERT-2017-1236, DFN-CERT:DFN-CERT-2016-1929, DFN-CERT:DFN-CERT-2016-1527, DFN-CERT:DFN-CERT-2016-1468, DFN-CERT:DFN-CERT-2016-1216, DFN-CERT:DFN-CERT-2016-1174, DFN-CERT:DFN-CERT-2016-1168, DFN-CERT:DFN-CERT-2016-0884, DFN-CERT:DFN-CERT-2016-0841, DFN-CERT:DFN-CERT-2016-0644, DFN-CERT:DFN-CERT-2016-0642, DFN-CERT:DFN-CERT-2016-0496, DFN-CERT:DFN-CERT-2016-0495, DFN-CERT:DFN-CERT-2016-0465, DFN-CERT:DFN-CERT-2016-0459, DFN-CERT:DFN-CERT-2016-0453, DFN-CERT:DFN-CERT-2016-0451, DFN-CERT:DFN-CERT-2016-0415, DFN-CERT:DFN-CERT-2016-0403, DFN-CERT:DFN-CERT-2016-0388, DFN-CERT:DFN-CERT-2016-0360, DFN-CERT:DFN-CERT-2016-0359, DFN-CERT:DFN-CERT-2016-0357, DFN-CERT:DFN-CERT-2016-0171, DFN-CERT:DFN-CERT-2015-1431, DFN-CERT:DFN-CERT-2015-1075, DFN-CERT:DFN-CERT-2015-1026, DFN-CERT:DFN-CERT-2015-0664, DFN-

CERT:DFN-CERT-2015-0548, DFN-CERT:DFN-CERT-2015-0404, DFN-CERT:DFN-CERT-2015-0396, DFN-CERT:DFN-CERT-2015-0259, DFN-CERT:DFN-CERT-2015-0254, DFN-CERT:DFN-CERT-2015-0245, DFN-CERT:DFN-CERT-2015-0118, DFN-CERT:DFN-CERT-2015-0114, DFN-CERT:DFN-CERT-2015-0083, DFN-CERT:DFN-CERT-2015-0082, DFN-CERT:DFN-CERT-2015-0081, DFN-CERT:DFN-CERT-2015-0076, DFN-CERT:DFN-CERT-2014-1717, DFN-CERT:DFN-CERT-2014-1680, DFN-CERT:DFN-CERT-2014-1632, DFN-CERT:DFN-CERT-2014-1564, DFN-CERT:DFN-CERT-2014-1542, DFN-CERT:DFN-CERT-2014-1414, DFN-CERT:DFN-CERT-2014-1366, DFN-CERT:DFN-CERT-2014-1354

## Scanner evidence for A19

The action above covers the following detailed scanner evidence.

**Vendor references**

CERT-BUND:WID-SEC-2026-0180, CERT-BUND:WID-SEC-2023-1435, CERT-BUND:CB-K18/0799, CERT-BUND:CB-K16/1289, CERT-BUND:CB-K16/1096, CERT-BUND:CB-K15/1751, CERT-BUND:CB-K15/1266, CERT-BUND:CB-K15/0850, CERT-BUND:CB-K15/0764, CERT-BUND:CB-K15/0720, CERT-BUND:CB-K15/0548, CERT-BUND:CB-K15/0526, CERT-BUND:CB-K15/0509, CERT-BUND:CB-K15/0493, CERT-BUND:CB-K15/0384, CERT-BUND:CB-K15/0365, CERT-BUND:CB-K15/0364, CERT-BUND:CB-K15/0302, CERT-BUND:CB-K15/0192, CERT-BUND:CB-K15/0079, CERT-BUND:CB-K15/0016, CERT-BUND:CB-K14/1342, CERT-BUND:CB-K14/0231, CERT-BUND:CB-K13/0845, CERT-BUND:CB-K13/0796, CERT-BUND:CB-K13/0790, DFN-CERT:DFN-CERT-2020-0177, DFN-CERT:DFN-CERT-2020-0111, DFN-CERT:DFN-CERT-2019-0068, DFN-CERT:DFN-CERT-2018-1441, DFN-CERT:DFN-CERT-2018-1408, DFN-CERT:DFN-CERT-2016-1372, DFN-CERT:DFN-CERT-2016-1164, DFN-CERT:DFN-CERT-2016-0388, DFN-CERT:DFN-CERT-2015-1853, DFN-CERT:DFN-CERT-2015-1332, DFN-CERT:DFN-CERT-2015-0884, DFN-CERT:DFN-CERT-2015-0800, DFN-CERT:DFN-CERT-2015-0758, DFN-CERT:DFN-CERT-2015-0567, DFN-CERT:DFN-CERT-2015-0544, DFN-CERT:DFN-CERT-2015-0530, DFN-CERT:DFN-CERT-2015-0396, DFN-CERT:DFN-CERT-2015-0375, DFN-CERT:DFN-CERT-2015-0374, DFN-CERT:DFN-CERT-2015-0305, DFN-CERT:DFN-CERT-2015-0199, DFN-CERT:DFN-CERT-2015-0079, DFN-CERT:DFN-CERT-2015-0021, DFN-CERT:DFN-CERT-2014-1414, DFN-CERT:DFN-CERT-2013-1847, DFN-CERT:DFN-CERT-2013-1792, DFN-CERT:DFN-CERT-2012-1979, DFN-CERT:DFN-CERT-2012-1829, DFN-CERT:DFN-CERT-2012-1530, DFN-CERT:DFN-CERT-2012-1380, DFN-CERT:DFN-CERT-2012-1377, DFN-CERT:DFN-CERT-2012-1292, DFN-CERT:DFN-CERT-2012-1214, DFN-CERT:DFN-CERT-2012-1213, DFN-CERT:DFN-CERT-2012-1180, DFN-CERT:DFN-CERT-2012-1156, DFN-CERT:DFN-CERT-2012-1155, DFN-CERT:DFN-CERT-2012-1039, DFN-CERT:DFN-CERT-2012-0956, DFN-CERT:DFN-CERT-2012-0908, DFN-CERT:DFN-CERT-2012-0868, DFN-CERT:DFN-CERT-2012-0867, DFN-CERT:DFN-CERT-2012-0848, DFN-CERT:DFN-CERT-2012-0838, DFN-CERT:DFN-CERT-2012-0776, DFN-CERT:DFN-CERT-2012-0722, DFN-CERT:DFN-CERT-2012-0638, DFN-CERT:DFN-CERT-2012-0627, DFN-CERT:DFN-CERT-2012-0451, DFN-CERT:DFN-CERT-2012-0418, DFN-CERT:DFN-CERT-2012-0354, DFN-CERT:DFN-CERT-2012-0234, DFN-CERT:DFN-CERT-2012-0221, DFN-CERT:DFN-CERT-2012-0177, DFN-CERT:DFN-CERT-2012-0170, DFN-CERT:DFN-CERT-2012-0146, DFN-CERT:DFN-CERT-2012-0142, DFN-CERT:DFN-CERT-2012-0126, DFN-CERT:DFN-CERT-2012-0123, DFN-CERT:DFN-CERT-2012-0095, DFN-CERT:DFN-CERT-2012-0051, DFN-CERT:DFN-CERT-2012-0047, DFN-CERT:DFN-CERT-2012-0021, DFN-CERT:DFN-CERT-2011-1953, DFN-CERT:DFN-CERT-2011-1946, DFN-CERT:DFN-CERT-2011-1844, DFN-CERT:DFN-CERT-2011-1826, DFN-CERT:DFN-CERT-2011-1774, DFN-CERT:DFN-CERT-2011-1743, DFN-CERT:DFN-CERT-2011-1738, DFN-CERT:DFN-CERT-2011-1706, DFN-CERT:DFN-CERT-2011-1628, DFN-CERT:DFN-CERT-2011-1627, DFN-CERT:DFN-CERT-2011-1619, DFN-CERT:DFN-CERT-2011-1482

## Scanner evidence for A20

The action above covers the following detailed scanner evidence.

**Vendor references**

CERT-BUND:WID-SEC-2024-3056, CERT-BUND:WID-SEC-2023-1886, CERT-BUND:WID-SEC-2023-1352, CERT-BUND:WID-SEC-2022-2251, CERT-BUND:WID-SEC-2022-2000, CERT-

| | |
|---|---|
| | BUND:CB-K22/0224, CERT-BUND:CB-K21/1276, DFN-CERT:DFN-CERT-2026-2722, DFN-CERT:DFN-CERT-2025-3324, DFN-CERT:DFN-CERT-2024-2847, DFN-CERT:DFN-CERT-2024-2578, DFN-CERT:DFN-CERT-2024-1671, DFN-CERT:DFN-CERT-2023-1697, DFN-CERT:DFN-CERT-2023-1332, DFN-CERT:DFN-CERT-2022-2147, DFN-CERT:DFN-CERT-2022-0437, DFN-CERT:DFN-CERT-2021-2622 |

## Scanner evidence for A25

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2026-2904, CERT-BUND:WID-SEC-2026-0180, CERT-BUND:WID-SEC-2024-1591, CERT-BUND:WID-SEC-2024-0796, CERT-BUND:WID-SEC-2023-1435, CERT-BUND:CB-K17/0980, CERT-BUND:CB-K17/0979, CERT-BUND:CB-K14/0772, CERT-BUND:CB-K13/0915, CERT-BUND:CB-K13/0462, DFN-CERT:DFN-CERT-2025-0933, DFN-CERT:DFN-CERT-2017-1013, DFN-CERT:DFN-CERT-2017-1012, DFN-CERT:DFN-CERT-2014-0809, DFN-CERT:DFN-CERT-2013-1928, DFN-CERT:DFN-CERT-2012-1112 |

## Scanner evidence for A28

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2011-0700, DFN-CERT:DFN-CERT-2010-1665, DFN-CERT:DFN-CERT-2010-1647, DFN-CERT:DFN-CERT-2009-1725, DFN-CERT:DFN-CERT-2009-1507, DFN-CERT:DFN-CERT-2009-1225 |

## Scanner evidence for A29

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2012-1293, DFN-CERT:DFN-CERT-2009-1748, DFN-CERT:DFN-CERT-2009-1528, DFN-CERT:DFN-CERT-2009-1508, DFN-CERT:DFN-CERT-2009-1452, DFN-CERT:DFN-CERT-2009-1409, DFN-CERT:DFN-CERT-2009-1408, DFN-CERT:DFN-CERT-2009-1393, DFN-CERT:DFN-CERT-2009-1381, DFN-CERT:DFN-CERT-2009-1380, DFN-CERT:DFN-CERT-2009-1340 |

## Scanner evidence for A30

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2010-0482, DFN-CERT:DFN-CERT-2010-0157, DFN-CERT:DFN-CERT-2010-0133, DFN-CERT:DFN-CERT-2009-1708, DFN-CERT:DFN-CERT-2009-1632, DFN-CERT:DFN-CERT-2009-1621, DFN-CERT:DFN-CERT-2009-1523, DFN-CERT:DFN-CERT-2009-1522, DFN-CERT:DFN-CERT-2009-1508, DFN-CERT:DFN-CERT-2009-1455, DFN-CERT:DFN-CERT-2009-1439, DFN-CERT:DFN-CERT-2009-1399 |

## Scanner evidence for A31

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2009-1508, DFN-CERT:DFN-CERT-2009-1503, DFN-CERT:DFN-CERT-2009-1463 |

## Scanner evidence for A32

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2009-1633, DFN-CERT:DFN-CERT-2009-1539 |

## Scanner evidence for A33

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2010-1227, DFN-CERT:DFN-CERT-2010-0802, DFN-CERT:DFN-CERT-2010-0263, DFN-CERT:DFN-CERT-2010-0143, DFN-CERT:DFN-CERT-2010-0140, DFN-CERT:DFN-CERT-2010-0060, DFN-CERT:DFN-CERT-2009-1726, DFN-CERT:DFN-CERT-2009-1666, DFN-CERT:DFN-CERT-2009-1663, DFN-CERT:DFN-CERT-2009-1639 |

## Scanner evidence for A34

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2012-1293, DFN-CERT:DFN-CERT-2010-0682, DFN-CERT:DFN-CERT-2010-0681, DFN-CERT:DFN-CERT-2010-0680, DFN-CERT:DFN-CERT-2010-0085, DFN-CERT:DFN-CERT-2010-0007, DFN-CERT:DFN-CERT-2010-0001, DFN-CERT:DFN-CERT-2009-1799, DFN-CERT:DFN-CERT-2009-1791 |

## Scanner evidence for A35

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2010-0698, DFN-CERT:DFN-CERT-2010-0689, DFN-CERT:DFN-CERT-2010-0682, DFN-CERT:DFN-CERT-2010-0681, DFN-CERT:DFN-CERT-2010-0680 |

## Scanner evidence for A36

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2012-0462, DFN-CERT:DFN-CERT-2012-0171, DFN-CERT:DFN-CERT-2011-1306, DFN-CERT:DFN-CERT-2010-0984, DFN-CERT:DFN-CERT-2010-0842, DFN-CERT:DFN-CERT-2010-0641, DFN-CERT:DFN-CERT-2010-0639, DFN-CERT:DFN-CERT-2010-0275, DFN-CERT:DFN-CERT-2010-0268, DFN-CERT:DFN-CERT-2010-0266, DFN-CERT:DFN-CERT-2010-0218, DFN-CERT:DFN-CERT-2010-0198, DFN-CERT:DFN-CERT-2010-0155, DFN-CERT:DFN-CERT-2010-0136, DFN-CERT:DFN-CERT-2010-0134, DFN-CERT:DFN-CERT-2010-0133, DFN-CERT:DFN-CERT-2010-0129 |

## Scanner evidence for A37

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2010-1620, DFN-CERT:DFN-CERT-2010-1247, DFN-CERT:DFN-CERT-2010-1079, DFN-CERT:DFN-CERT-2010-0953, DFN-CERT:DFN-CERT-2010-0775, DFN-CERT:DFN-CERT-2010-0705, DFN-CERT:DFN-CERT-2010-0419, DFN-CERT:DFN-CERT-2010-0372 |

## Scanner evidence for A38

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2009-1497 |

## Scanner evidence for A39

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2009-1497 |

## Scanner evidence for A40

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2010-0624 |

## Scanner evidence for A42

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2012-0462, DFN-CERT:DFN-CERT-2010-0954 |

## Scanner evidence for A43

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K15/1514, DFN-CERT:DFN-CERT-2012-1293, DFN-CERT:DFN-CERT-2011-1011, DFN-CERT:DFN-CERT-2010-1430, DFN-CERT:DFN-CERT-2010-1135, DFN-CERT:DFN-CERT-2010-1117, DFN-CERT:DFN-CERT-2010-1046, DFN-CERT:DFN-CERT-2010-0984, DFN-CERT:DFN-CERT-2010-0976, DFN-CERT:DFN-CERT-2010-0774, DFN-CERT:DFN-CERT-2010-0773, DFN-CERT:DFN-CERT-2010-0740, DFN-CERT:DFN-CERT-2010-0698, DFN-CERT:DFN-CERT-2010-0689, DFN-CERT:DFN-CERT-2010-0683, DFN-CERT:DFN-CERT-2010-0682, DFN-CERT:DFN-CERT-2010-0681, DFN-CERT:DFN-CERT-2010-0680, DFN-CERT:DFN-CERT-2010-0673 |

## Scanner evidence for A44

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2012-1293, DFN-CERT:DFN-CERT-2010-0984, DFN-CERT:DFN-CERT-2010-0698, DFN-CERT:DFN-CERT-2010-0689 |

## Scanner evidence for A45

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2012-0462, DFN-CERT:DFN-CERT-2011-0962, DFN-CERT:DFN-CERT-2010-1643, DFN-CERT:DFN-CERT-2010-1135, DFN-CERT:DFN-CERT-2010-0984, DFN-CERT:DFN-CERT-2010-0842, DFN-CERT:DFN-CERT-2010-0799, DFN-CERT:DFN-CERT-2010-0794, DFN-CERT:DFN-CERT-2010-0789 |

## Scanner evidence for A46

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2011-1005, DFN-CERT:DFN-CERT-2011-0642, DFN-CERT:DFN-CERT-2010-1620, DFN-CERT:DFN-CERT-2010-1321, DFN-CERT:DFN-CERT-2010-1247, DFN-CERT:DFN-CERT-2010-1079, DFN-CERT:DFN-CERT-2010-0997, DFN-CERT:DFN-CERT-2010-0953 |

## Scanner evidence for A47

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2012-0731, DFN-CERT:DFN-CERT-2012-0618, DFN-CERT:DFN-CERT-2011-1693, DFN-CERT:DFN-CERT-2011-1342, DFN-CERT:DFN-CERT-2011-1341, DFN-CERT:DFN-CERT-2011-1298, DFN-CERT:DFN-CERT-2011-0700, DFN-CERT:DFN- |

CERT-2010-1665, DFN-CERT:DFN-CERT-2010-1647, DFN-CERT:DFN-CERT-2010-1123, DFN-CERT:DFN-CERT-2010-1053, DFN-CERT:DFN-CERT-2010-1048, DFN-CERT:DFN-CERT-2010-1041

## Scanner evidence for A48

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2011-1005, DFN-CERT:DFN-CERT-2011-0642, DFN-CERT:DFN-CERT-2010-1620, DFN-CERT:DFN-CERT-2010-1321, DFN-CERT:DFN-CERT-2010-1247, DFN-CERT:DFN-CERT-2010-1079, DFN-CERT:DFN-CERT-2010-0997, DFN-CERT:DFN-CERT-2010-0953 |

## Scanner evidence for A49

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2010-1191, DFN-CERT:DFN-CERT-2010-1121, DFN-CERT:DFN-CERT-2010-1119, DFN-CERT:DFN-CERT-2010-1102, DFN-CERT:DFN-CERT-2010-1085, DFN-CERT:DFN-CERT-2010-1077 |

## Scanner evidence for A51

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2012-0462, DFN-CERT:DFN-CERT-2011-0962, DFN-CERT:DFN-CERT-2011-0321, DFN-CERT:DFN-CERT-2011-0046, DFN-CERT:DFN-CERT-2010-1650, DFN-CERT:DFN-CERT-2010-1543, DFN-CERT:DFN-CERT-2010-1424, DFN-CERT:DFN-CERT-2010-1321, DFN-CERT:DFN-CERT-2010-1232, DFN-CERT:DFN-CERT-2010-1230, DFN-CERT:DFN-CERT-2010-1220, DFN-CERT:DFN-CERT-2010-1219, DFN-CERT:DFN-CERT-2010-1218 |

## Scanner evidence for A52

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K15/1514, DFN-CERT:DFN-CERT-2012-1293, DFN-CERT:DFN-CERT-2010-1604, DFN-CERT:DFN-CERT-2010-1492, DFN-CERT:DFN-CERT-2010-1430, DFN-CERT:DFN-CERT-2010-1424, DFN-CERT:DFN-CERT-2010-1389, DFN-CERT:DFN-CERT-2010-1379, DFN-CERT:DFN-CERT-2010-1346, DFN-CERT:DFN-CERT-2010-1316, DFN-CERT:DFN-CERT-2010-1310 |

## Scanner evidence for A53

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2011-0642, DFN-CERT:DFN-CERT-2011-0147, DFN-CERT:DFN-CERT-2010-1526 |

## Scanner evidence for A54

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2011-0002, DFN-CERT:DFN-CERT-2010-1662, DFN-CERT:DFN-CERT-2010-1625 |

## Scanner evidence for A55

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2012-0731, DFN-CERT:DFN-CERT-2012-0514, DFN-CERT:DFN-CERT-2011-0515, DFN-CERT:DFN-CERT-2011-0148, DFN-CERT:DFN-CERT-2011-0147, DFN-CERT:DFN-CERT-2011-0097, DFN-CERT:DFN-CERT-2011-0096, DFN-CERT:DFN-CERT-2011-0095 |

## Scanner evidence for A56

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K15/1514, DFN-CERT:DFN-CERT-2012-1293, DFN-CERT:DFN-CERT-2011-0492, DFN-CERT:DFN-CERT-2011-0176, DFN-CERT:DFN-CERT-2011-0151, DFN-CERT:DFN-CERT-2011-0149, DFN-CERT:DFN-CERT-2011-0146, DFN-CERT:DFN-CERT-2011-0143 |

## Scanner evidence for A57

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2011-0289, DFN-CERT:DFN-CERT-2011-0263, DFN-CERT:DFN-CERT-2011-0214, DFN-CERT:DFN-CERT-2011-0190 |

## Scanner evidence for A58

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2012-1981, DFN-CERT:DFN-CERT-2012-0627, DFN-CERT:DFN-CERT-2012-0462, DFN-CERT:DFN-CERT-2011-0962, DFN-CERT:DFN-CERT-2011-0712, DFN-CERT:DFN-CERT-2011-0399, DFN-CERT:DFN-CERT-2011-0274, DFN-CERT:DFN-CERT-2011-0268, DFN-CERT:DFN-CERT-2011-0267 |

## Scanner evidence for A60

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2012-0218, DFN-CERT:DFN-CERT-2011-1866, DFN-CERT:DFN-CERT-2011-1783, DFN-CERT:DFN-CERT-2011-1764 |

## Scanner evidence for A62

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2013-1494, DFN-CERT:DFN-CERT-2012-1268, DFN-CERT:DFN-CERT-2012-1267, DFN-CERT:DFN-CERT-2012-1266, DFN-CERT:DFN-CERT-2012-1173, DFN-CERT:DFN-CERT-2012-0914, DFN-CERT:DFN-CERT-2012-0907, DFN-CERT:DFN-CERT-2012-0906, DFN-CERT:DFN-CERT-2012-0900, DFN-CERT:DFN-CERT-2012-0870, DFN-CERT:DFN-CERT-2012-0869, DFN-CERT:DFN-CERT-2012-0866, DFN-CERT:DFN-CERT-2012-0813, DFN-CERT:DFN-CERT-2012-0773 |

## Scanner evidence for A64

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2019-0381 |

## Scanner evidence for A65

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K15/1514, DFN-CERT:DFN-CERT-2011-0917, DFN-CERT:DFN-CERT-2011-0912, DFN-CERT:DFN-CERT-2011-0897, DFN-CERT:DFN-CERT-2011-0844, DFN-CERT:DFN-CERT-2011-0818, DFN-CERT:DFN-CERT-2011-0808, DFN-CERT:DFN-CERT-2011-0771, DFN-CERT:DFN-CERT-2011-0741, DFN-CERT:DFN-CERT-2011-0712, DFN-CERT:DFN-CERT-2011-0673, DFN-CERT:DFN-CERT-2011-0597, DFN-CERT:DFN-CERT-2011-0596, DFN-CERT:DFN-CERT-2011-0519, DFN-CERT:DFN-CERT-2011-0516, DFN-CERT:DFN- |

CERT-2011-0483, DFN-CERT:DFN-CERT-2011-0434, DFN-CERT:DFN-CERT-2011-0393, DFN-CERT:DFN-CERT-2011-0381

## Scanner evidence for A66

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2012-1211 |

## Scanner evidence for A67

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K15/1266, CERT-BUND:CB-K15/0080, CERT-BUND:CB-K14/1423, CERT-BUND:CB-K13/0953, CERT-BUND:CB-K13/0943, DFN-CERT:DFN-CERT-2015-1332, DFN-CERT:DFN-CERT-2015-0082, DFN-CERT:DFN-CERT-2014-1491, DFN-CERT:DFN-CERT-2013-1971, DFN-CERT:DFN-CERT-2013-1967, DFN-CERT:DFN-CERT-2013-1307, DFN-CERT:DFN-CERT-2013-0944, DFN-CERT:DFN-CERT-2013-0742, DFN-CERT:DFN-CERT-2013-0397, DFN-CERT:DFN-CERT-2013-0298 |

## Scanner evidence for A68

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2022-0842, DFN-CERT:DFN-CERT-2024-1065, DFN-CERT:DFN-CERT-2023-0713, DFN-CERT:DFN-CERT-2023-0199, DFN-CERT:DFN-CERT-2023-0153, DFN-CERT:DFN-CERT-2023-0089, DFN-CERT:DFN-CERT-2022-2804, DFN-CERT:DFN-CERT-2022-2514, DFN-CERT:DFN-CERT-2022-1686, DFN-CERT:DFN-CERT-2022-1674, DFN-CERT:DFN-CERT-2022-1662 |

## Scanner evidence for A69

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2023-1737, CERT-BUND:WID-SEC-2023-0561, CERT-BUND:WID-SEC-2023-0137, CERT-BUND:WID-SEC-2022-1567, DFN-CERT:DFN-CERT-2024-1192, DFN-CERT:DFN-CERT-2023-1600, DFN-CERT:DFN-CERT-2023-0422, DFN-CERT:DFN-CERT-2022-2869, DFN-CERT:DFN-CERT-2022-2639, DFN-CERT:DFN-CERT-2022-2638, DFN-CERT:DFN-CERT-2022-2598, DFN-CERT:DFN-CERT-2022-2523, DFN-CERT:DFN-CERT-2022-2337, DFN-CERT:DFN-CERT-2022-2157 |

## Scanner evidence for A70

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2024-0794, CERT-BUND:WID-SEC-2023-2690, CERT-BUND:WID-SEC-2023-2031, CERT-BUND:WID-SEC-2023-1812, CERT-BUND:WID-SEC-2023-1737, CERT-BUND:WID-SEC-2023-1542, CERT-BUND:WID-SEC-2023-1424, CERT-BUND:WID-SEC-2023-1021, CERT-BUND:WID-SEC-2022-2372, CERT-BUND:WID-SEC-2022-2057, DFN-CERT:DFN-CERT-2025-1637, DFN-CERT:DFN-CERT-2023-2536, DFN-CERT:DFN-CERT-2023-1592, DFN-CERT:DFN-CERT-2023-1230, DFN-CERT:DFN-CERT-2023-1162, DFN-CERT:DFN-CERT-2023-0199, DFN-CERT:DFN-CERT-2023-0089, DFN-CERT:DFN-CERT-2022-2804, DFN-CERT:DFN-CERT-2022-2657, DFN-CERT:DFN-CERT-2022-2612, DFN-CERT:DFN-CERT-2022-2603, DFN-CERT:DFN-CERT-2022-2579 |

## Scanner evidence for A71

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2022-2365, DFN-CERT:DFN-CERT-2025-1637, DFN-CERT:DFN-CERT-2022-2870 |

## Scanner evidence for A72

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2024-0064, CERT-BUND:WID-SEC-2023-1737, CERT-BUND:WID-SEC-2022-2365, CERT-BUND:WID-SEC-2022-1983, DFN-CERT:DFN-CERT-2023-1592, DFN-CERT:DFN-CERT-2023-1311, DFN-CERT:DFN-CERT-2023-1162, DFN-CERT:DFN-CERT-2023-0286, DFN-CERT:DFN-CERT-2023-0201, DFN-CERT:DFN-CERT-2023-0199, DFN-CERT:DFN-CERT-2023-0176, DFN-CERT:DFN-CERT-2023-0153, DFN-CERT:DFN-CERT-2023-0089, DFN-CERT:DFN-CERT-2022-2870, DFN-CERT:DFN-CERT-2022-2429 |

## Scanner evidence for A74

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2023-2671, CERT-BUND:WID-SEC-2023-1424, CERT-BUND:WID-SEC-2023-1022, CERT-BUND:WID-SEC-2023-0383, DFN-CERT:DFN-CERT-2024-3330, DFN-CERT:DFN-CERT-2024-2681, DFN-CERT:DFN-CERT-2023-2570, DFN-CERT:DFN-CERT-2023-2538, DFN-CERT:DFN-CERT-2023-0994, DFN-CERT:DFN-CERT-2023-0884, DFN-CERT:DFN-CERT-2023-0462, DFN-CERT:DFN-CERT-2023-0435, DFN-CERT:DFN-CERT-2023-0336 |

## Scanner evidence for A76

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2023-0695, DFN-CERT:DFN-CERT-2024-2707, DFN-CERT:DFN-CERT-2024-1132, DFN-CERT:DFN-CERT-2023-0681 |

## Scanner evidence for A77

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2023-2910, CERT-BUND:WID-SEC-2023-1842, DFN-CERT:DFN-CERT-2025-1637, DFN-CERT:DFN-CERT-2024-1661, DFN-CERT:DFN-CERT-2024-1065, DFN-CERT:DFN-CERT-2024-0839, DFN-CERT:DFN-CERT-2024-0519, DFN-CERT:DFN-CERT-2024-0231, DFN-CERT:DFN-CERT-2023-2818, DFN-CERT:DFN-CERT-2023-1744, DFN-CERT:DFN-CERT-2023-1741, DFN-CERT:DFN-CERT-2023-1666 |

## Scanner evidence for A78

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2023-2620, DFN-CERT:DFN-CERT-2024-1065, DFN-CERT:DFN-CERT-2024-0839, DFN-CERT:DFN-CERT-2023-2700, DFN-CERT:DFN-CERT-2023-2494, DFN-CERT:DFN-CERT-2023-2462, DFN-CERT:DFN-CERT-2023-2447, DFN-CERT:DFN-CERT-2023-2443 |

## Scanner evidence for A79

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K15/1266, CERT-BUND:CB-K14/1399, DFN-CERT:DFN-CERT-2015-1332, DFN-CERT:DFN-CERT-2014-1479 |

## Scanner evidence for A80

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K15/1437, CERT-BUND:CB-K14/1399, CERT-BUND:CB-K14/0893, CERT-BUND:CB-K14/0400, CERT-BUND:CB-K14/0345, DFN-CERT:DFN-CERT-2015-1514, DFN-CERT:DFN-CERT-2014-1479, DFN-CERT:DFN-CERT-2014-0922, DFN-CERT:DFN-CERT-2014-0415, DFN-CERT:DFN-CERT-2014-0360 |

## Scanner evidence for A81

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K15/1105, CERT-BUND:CB-K15/0299, CERT-BUND:CB-K14/1399, CERT-BUND:CB-K14/0407, CERT-BUND:CB-K14/0400, DFN-CERT:DFN-CERT-2015-1161, DFN-CERT:DFN-CERT-2015-0303, DFN-CERT:DFN-CERT-2014-1479, DFN-CERT:DFN-CERT-2014-0422, DFN-CERT:DFN-CERT-2014-0415 |

## Scanner evidence for A82

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2026-0180, CERT-BUND:WID-SEC-2023-0500, CERT-BUND:CB-K15/0567, CERT-BUND:CB-K15/0415, CERT-BUND:CB-K15/0384, CERT-BUND:CB-K15/0080, CERT-BUND:CB-K15/0079, CERT-BUND:CB-K15/0074, CERT-BUND:CB-K14/1617, CERT-BUND:CB-K14/1537, CERT-BUND:CB-K14/1299, CERT-BUND:CB-K14/1297, CERT-BUND:CB-K14/1294, CERT-BUND:CB-K14/1202, CERT-BUND:CB-K14/1174, CERT-BUND:CB-K14/1153, CERT-BUND:CB-K14/0876, CERT-BUND:CB-K14/0756, CERT-BUND:CB-K14/0746, CERT-BUND:CB-K14/0736, CERT-BUND:CB-K14/0722, CERT-BUND:CB-K14/0716, CERT-BUND:CB-K14/0708, CERT-BUND:CB-K14/0684, CERT-BUND:CB-K14/0683, CERT-BUND:CB-K14/0680, DFN-CERT:DFN-CERT-2016-0388, DFN-CERT:DFN-CERT-2015-0593, DFN-CERT:DFN-CERT-2015-0427, DFN-CERT:DFN-CERT-2015-0396, DFN-CERT:DFN-CERT-2015-0082, DFN-CERT:DFN-CERT-2015-0079, DFN-CERT:DFN-CERT-2015-0078, DFN-CERT:DFN-CERT-2014-1717, DFN-CERT:DFN-CERT-2014-1632, DFN-CERT:DFN-CERT-2014-1364, DFN-CERT:DFN-CERT-2014-1357, DFN-CERT:DFN-CERT-2014-1350, DFN-CERT:DFN-CERT-2014-1265, DFN-CERT:DFN-CERT-2014-1209, DFN-CERT:DFN-CERT-2014-0917, DFN-CERT:DFN-CERT-2014-0789, DFN-CERT:DFN-CERT-2014-0778, DFN-CERT:DFN-CERT-2014-0768, DFN-CERT:DFN-CERT-2014-0752, DFN-CERT:DFN-CERT-2014-0747, DFN-CERT:DFN-CERT-2014-0738, DFN-CERT:DFN-CERT-2014-0715, DFN-CERT:DFN-CERT-2014-0714, DFN-CERT:DFN-CERT-2014-0709 |

## Scanner evidence for A83

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K16/0596, CERT-BUND:CB-K16/0572, CERT-BUND:CB-K15/0245, CERT-BUND:CB-K15/0230, DFN-CERT:DFN-CERT-2016-0648, DFN-CERT:DFN-CERT-2016-0620, DFN-CERT:DFN-CERT-2015-0253, DFN-CERT:DFN-CERT-2015-0237 |

## Scanner evidence for A85

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K20/0857, CERT-BUND:CB-K19/0961, DFN-CERT:DFN-CERT-2020-0072, DFN-CERT:DFN-CERT-2019-2189 |

## Scanner evidence for A88

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K15/0130, DFN-CERT:DFN-CERT-2015-0130 |

## Scanner evidence for A89

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2023-2718, CERT-BUND:CB-K17/1957, CERT-BUND:CB-K17/1575, CERT-BUND:CB-K17/1461, CERT-BUND:CB-K17/1358, CERT-BUND:CB-K17/1252, CERT-BUND:CB-K17/0527, CERT-BUND:CB-K17/0327, CERT-BUND:CB-K17/0318, CERT-BUND:CB-K17/0269, CERT-BUND:CB-K17/0264, CERT-BUND:CB-K17/0232, CERT-BUND:CB-K17/0182, CERT-BUND:CB-K17/0141, DFN-CERT:DFN-CERT-2018-0835, DFN-CERT:DFN-CERT-2017-2044, DFN-CERT:DFN-CERT-2017-1647, DFN-CERT:DFN-CERT-2017-1529, DFN-CERT:DFN-CERT-2017-1420, DFN-CERT:DFN-CERT-2017-1295, DFN-CERT:DFN-CERT-2017-0532, DFN-CERT:DFN-CERT-2017-0334, DFN-CERT:DFN-CERT-2017-0325, DFN-CERT:DFN-CERT-2017-0274, DFN-CERT:DFN-CERT-2017-0270, DFN-CERT:DFN-CERT-2017-0234, DFN-CERT:DFN-CERT-2017-0179, DFN-CERT:DFN-CERT-2017-0144 |

## Scanner evidence for A90

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2011-1222, DFN-CERT:DFN-CERT-2011-1168, DFN-CERT:DFN-CERT-2011-1132, DFN-CERT:DFN-CERT-2011-1130 |

## Scanner evidence for A91

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2023-1594, CERT-BUND:CB-K18/1012, CERT-BUND:CB-K18/0800, CERT-BUND:CB-K18/0606, CERT-BUND:CB-K18/0098, CERT-BUND:CB-K18/0066, CERT-BUND:CB-K17/2188, CERT-BUND:CB-K17/2117, CERT-BUND:CB-K17/2021, CERT-BUND:CB-K17/1980, CERT-BUND:CB-K17/1936, CERT-BUND:CB-K17/1871, CERT-BUND:CB-K17/1773, CERT-BUND:CB-K17/1768, CERT-BUND:CB-K17/1587, DFN-CERT:DFN-CERT-2019-0359, DFN-CERT:DFN-CERT-2018-2113, DFN-CERT:DFN-CERT-2018-1070, DFN-CERT:DFN-CERT-2018-0725, DFN-CERT:DFN-CERT-2018-0100, DFN-CERT:DFN-CERT-2018-0077, DFN-CERT:DFN-CERT-2017-2290, DFN-CERT:DFN-CERT-2017-2211, DFN-CERT:DFN-CERT-2017-2108, DFN-CERT:DFN-CERT-2017-2070, DFN-CERT:DFN-CERT-2017-2021, DFN-CERT:DFN-CERT-2017-1954, DFN-CERT:DFN-CERT-2017-1854, DFN-CERT:DFN-CERT-2017-1843, DFN-CERT:DFN-CERT-2017-1659 |

## Scanner evidence for A92

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2022-2128, CERT-BUND:CB-K18/1154, DFN-CERT:DFN-CERT-2022-2638, DFN-CERT:DFN-CERT-2019-1181, DFN-CERT:DFN-CERT-2019-0313, DFN-CERT:DFN-CERT-2019-0044, DFN-CERT:DFN-CERT-2018-2476 |

## Scanner evidence for A93

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2024-1086, CERT-BUND:WID-SEC-2024-0218, CERT-BUND:CB-K20/1030, DFN-CERT:DFN-CERT-2024-0233, DFN-CERT:DFN-CERT-2022-2107, DFN-CERT:DFN-CERT-2020-2412, DFN-CERT:DFN-CERT-2020-2105, DFN-CERT:DFN-CERT-2020-1964, DFN-CERT:DFN-CERT-2019-1804, DFN-CERT:DFN-CERT-2019-1471, DFN-CERT:DFN-CERT-2019-1424 |

## Scanner evidence for A96

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2022-0418, CERT-BUND:CB-K20/0081, CERT-BUND:CB-K19/0943, DFN-CERT:DFN-CERT-2022-2638, DFN-CERT:DFN-CERT-2020-0415, DFN-CERT:DFN-CERT-2020-0193, DFN-CERT:DFN-CERT-2019-2283, DFN-CERT:DFN-CERT-2019-2206 |

## Scanner evidence for A97

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K14/0981, DFN-CERT:DFN-CERT-2021-1825, DFN-CERT:DFN-CERT-2014-1018, DFN-CERT:DFN-CERT-2010-0020 |

## Scanner evidence for A98

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K18/1080, DFN-CERT:DFN-CERT-2019-1285, DFN-CERT:DFN-CERT-2018-2290 |

## Scanner evidence for A99

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K20/0251, DFN-CERT:DFN-CERT-2020-2366, DFN-CERT:DFN-CERT-2020-0998, DFN-CERT:DFN-CERT-2020-0592 |

## Scanner evidence for A100

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K18/0877, DFN-CERT:DFN-CERT-2018-1704 |

## Scanner evidence for A101

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K20/0857, CERT-BUND:CB-K20/0163, DFN-CERT:DFN-CERT-2020-1078, DFN-CERT:DFN-CERT-2020-0361 |

## Scanner evidence for A102

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2023-2464, CERT-BUND:CB-K21/0172, DFN-CERT:DFN-CERT-2021-0324 |

## Scanner evidence for A103

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2025-0137, CERT-BUND:WID-SEC-2024-3116, CERT-BUND:WID-SEC-2024-2230, DFN-CERT:DFN-CERT-2025-1211, DFN-CERT:DFN-CERT-2025-0168, DFN-CERT:DFN-CERT-2024-3330, DFN-CERT:DFN-CERT-2024-3329, DFN-CERT:DFN-CERT-2024-2707, DFN-CERT:DFN-CERT-2024-2591, DFN-CERT:DFN-CERT-2024-2550 |

## Scanner evidence for A104

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2023-1737, CERT-BUND:WID-SEC-2022-1577, CERT-BUND:WID-SEC-2022-0624, CERT-BUND:CB-K21/0705, DFN-CERT:DFN-CERT-2023-1600, DFN-CERT:DFN- |

CERT-2022-2639, DFN-CERT:DFN-CERT-2022-2638, DFN-CERT:DFN-CERT-2022-1046, DFN-CERT:DFN-CERT-2021-2185, DFN-CERT:DFN-CERT-2021-1676, DFN-CERT:DFN-CERT-2021-1645, DFN-CERT:DFN-CERT-2021-1627, DFN-CERT:DFN-CERT-2021-1509, DFN-CERT:DFN-CERT-2021-1453, DFN-CERT:DFN-CERT-2021-1419

## Scanner evidence for A105

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2022-2112, CERT-BUND:CB-K21/1008, DFN-CERT:DFN-CERT-2022-2639, DFN-CERT:DFN-CERT-2021-2474, DFN-CERT:DFN-CERT-2021-1994 |

## Scanner evidence for A106

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2023-1542, CERT-BUND:WID-SEC-2022-2280, CERT-BUND:WID-SEC-2022-0432, CERT-BUND:WID-SEC-2022-0302, CERT-BUND:CB-K21/1126, CERT-BUND:CB-K20/1109, DFN-CERT:DFN-CERT-2024-0078, DFN-CERT:DFN-CERT-2023-1053, DFN-CERT:DFN-CERT-2022-1686, DFN-CERT:DFN-CERT-2022-0332, DFN-CERT:DFN-CERT-2020-2464 |

## Scanner evidence for A107

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2023-2366, CERT-BUND:CB-K19/0945, DFN-CERT:DFN-CERT-2023-2166, DFN-CERT:DFN-CERT-2021-1167, DFN-CERT:DFN-CERT-2020-2026, DFN-CERT:DFN-CERT-2020-1078, DFN-CERT:DFN-CERT-2020-0891, DFN-CERT:DFN-CERT-2020-0657, DFN-CERT:DFN-CERT-2020-0600, DFN-CERT:DFN-CERT-2020-0375, DFN-CERT:DFN-CERT-2019-2244, DFN-CERT:DFN-CERT-2019-2240 |

## Scanner evidence for A108

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2024-1082, CERT-BUND:WID-SEC-2024-0872, CERT-BUND:WID-SEC-2023-1995, CERT-BUND:WID-SEC-2023-0561, CERT-BUND:CB-K19/0627, CERT-BUND:CB-K19/0312, CERT-BUND:CB-K19/0058, CERT-BUND:CB-K19/0037, DFN-CERT:DFN-CERT-2024-1260, DFN-CERT:DFN-CERT-2019-2157, DFN-CERT:DFN-CERT-2019-1470, DFN-CERT:DFN-CERT-2019-0970, DFN-CERT:DFN-CERT-2019-0776, DFN-CERT:DFN-CERT-2019-0563, DFN-CERT:DFN-CERT-2019-0415, DFN-CERT:DFN-CERT-2019-0357, DFN-CERT:DFN-CERT-2019-0275, DFN-CERT:DFN-CERT-2019-0136, DFN-CERT:DFN-CERT-2019-0094 |

## Scanner evidence for A110

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K17/0318, DFN-CERT:DFN-CERT-2017-0325 |

## Scanner evidence for A111

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K17/0527, CERT-BUND:CB-K17/0327, CERT-BUND:CB-K17/0269, CERT-BUND:CB-K17/0053, CERT-BUND:CB-K17/0015, CERT-BUND:CB-K16/2015, CERT-BUND:CB-K16/1982, DFN-CERT:DFN-CERT-2018-0835, DFN-CERT:DFN-CERT-2017-0532, DFN-CERT:DFN-CERT-2017-0334, DFN-CERT:DFN-CERT-2017-0274, DFN-CERT:DFN-CERT-2017-0058, DFN-CERT:DFN-CERT-2017-0016, DFN-CERT:DFN-CERT-2016-2130, DFN-CERT:DFN-CERT-2016-2084 |

## Scanner evidence for A112

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2026-1032, CERT-BUND:WID-SEC-2025-0810, CERT-BUND:WID-SEC-2025-0168, CERT-BUND:WID-SEC-2025-0144, CERT-BUND:WID-SEC-2025-0139, CERT-BUND:WID-SEC-2024-3377, CERT-BUND:WID-SEC-2024-3320, CERT-BUND:WID-SEC-2024-3198, CERT-BUND:WID-SEC-2024-3195, CERT-BUND:WID-SEC-2024-3140, CERT-BUND:WID-SEC-2024-1913, CERT-BUND:WID-SEC-2024-1781, CERT-BUND:WID-SEC-2024-1701, CERT-BUND:WID-SEC-2024-1656, CERT-BUND:WID-SEC-2024-1655, CERT-BUND:WID-SEC-2024-1643, CERT-BUND:WID-SEC-2024-1642, CERT-BUND:WID-SEC-2024-1639, CERT-BUND:WID-SEC-2024-1637, CERT-BUND:WID-SEC-2024-1630, CERT-BUND:WID-SEC-2024-1474, CERT-BUND:WID-SEC-2024-1248, CERT-BUND:WID-SEC-2024-1228, CERT-BUND:WID-SEC-2024-1186, CERT-BUND:WID-SEC-2024-1082, CERT-BUND:WID-SEC-2024-0899, CERT-BUND:WID-SEC-2024-0892, CERT-BUND:WID-SEC-2024-0889, CERT-BUND:WID-SEC-2024-0885, CERT-BUND:WID-SEC-2024-0874, CERT-BUND:WID-SEC-2024-0869, CERT-BUND:WID-SEC-2024-0578, CERT-BUND:WID-SEC-2024-0564, CERT-BUND:WID-SEC-2024-0523, CERT-BUND:WID-SEC-2023-3182, CERT-BUND:WID-SEC-2023-3174, DFN-CERT:DFN-CERT-2026-2378, DFN-CERT:DFN-CERT-2026-0392, DFN-CERT:DFN-CERT-2026-0097, DFN-CERT:DFN-CERT-2025-3629, DFN-CERT:DFN-CERT-2025-3272, DFN-CERT:DFN-CERT-2025-2058, DFN-CERT:DFN-CERT-2025-2037, DFN-CERT:DFN-CERT-2025-1447, DFN-CERT:DFN-CERT-2025-1177, DFN-CERT:DFN-CERT-2025-1025, DFN-CERT:DFN-CERT-2025-0660, DFN-CERT:DFN-CERT-2025-0502, DFN-CERT:DFN-CERT-2025-0294, DFN-CERT:DFN-CERT-2025-0173, DFN-CERT:DFN-CERT-2025-0165, DFN-CERT:DFN-CERT-2025-0024, DFN-CERT:DFN-CERT-2024-3171, DFN-CERT:DFN-CERT-2024-2818, DFN-CERT:DFN-CERT-2024-2759, DFN-CERT:DFN-CERT-2024-2741, DFN-CERT:DFN-CERT-2024-2682, DFN-CERT:DFN-CERT-2024-2602, DFN-CERT:DFN-CERT-2024-2573, DFN-CERT:DFN-CERT-2024-2392, DFN-CERT:DFN-CERT-2024-2210, DFN-CERT:DFN-CERT-2024-2209, DFN-CERT:DFN-CERT-2024-2194, DFN-CERT:DFN-CERT-2024-2169, DFN-CERT:DFN-CERT-2024-2048, DFN-CERT:DFN-CERT-2024-2030, DFN-CERT:DFN-CERT-2024-2028, DFN-CERT:DFN-CERT-2024-1930, DFN-CERT:DFN-CERT-2024-1895, DFN-CERT:DFN-CERT-2024-1869, DFN-CERT:DFN-CERT-2024-1868, DFN-CERT:DFN-CERT-2024-1865, DFN-CERT:DFN-CERT-2024-1862, DFN-CERT:DFN-CERT-2024-1854, DFN-CERT:DFN-CERT-2024-1846, DFN-CERT:DFN-CERT-2024-1817, DFN-CERT:DFN-CERT-2024-1794, DFN-CERT:DFN-CERT-2024-1715, DFN-CERT:DFN-CERT-2024-1698, DFN-CERT:DFN-CERT-2024-1688, DFN-CERT:DFN-CERT-2024-1655, DFN-CERT:DFN-CERT-2024-1600, DFN-CERT:DFN-CERT-2024-1443, DFN-CERT:DFN-CERT-2024-1442, DFN-CERT:DFN-CERT-2024-1413, DFN-CERT:DFN-CERT-2024-1382, DFN-CERT:DFN-CERT-2024-1380, DFN-CERT:DFN-CERT-2024-1373, DFN-CERT:DFN-CERT-2024-1260, DFN-CERT:DFN-CERT-2024-1259, DFN-CERT:DFN-CERT-2024-1108, DFN-CERT:DFN-CERT-2024-1061, DFN-CERT:DFN-CERT-2024-1029, DFN-CERT:DFN-CERT-2024-1003, DFN-CERT:DFN-CERT-2024-1000, DFN-CERT:DFN-CERT-2024-0896, DFN-CERT:DFN-CERT-2024-0779, DFN-CERT:DFN-CERT-2024-0762, DFN-CERT:DFN-CERT-2024-0744, DFN-CERT:DFN-CERT-2024-0698, DFN-CERT:DFN-CERT-2024-0633, DFN-CERT:DFN-CERT-2024-0619, DFN-CERT:DFN-CERT-2024-0618, DFN-CERT:DFN-CERT-2024-0616, DFN-CERT:DFN-CERT-2024-0597, DFN-CERT:DFN-CERT-2024-0545, DFN-CERT:DFN-CERT-2024-0526, DFN-CERT:DFN-CERT-2024-0491, DFN-CERT:DFN-CERT-2024-0480, DFN-CERT:DFN-CERT-2024-0451, DFN-CERT:DFN-CERT-2024-0440, DFN-CERT:DFN-CERT-2024-0420, DFN-CERT:DFN-CERT-2024-0388, DFN-CERT:DFN-CERT-2024-0343, DFN-CERT:DFN-CERT-2024-0306, DFN-CERT:DFN-CERT-2024-0299, DFN-CERT:DFN-CERT-2024-0285, DFN-CERT:DFN-CERT-2024-0267, DFN-CERT:DFN-CERT-2024-0251, DFN-CERT:DFN-CERT-2024-0215, DFN-CERT:DFN-CERT-2024-0211, DFN-CERT:DFN-CERT-2024-0164, DFN-CERT:DFN-CERT-2024-0154, DFN-CERT:DFN-CERT-2024-0101, DFN-CERT:DFN-CERT-2024-0092, DFN-CERT:DFN-CERT-2024-0088, DFN-CERT:DFN-CERT-2024-0067, DFN-CERT:DFN-CERT-2024-0063, DFN-CERT:DFN-CERT-2024-0062, DFN-CERT:DFN-CERT-2024-0024, DFN-CERT:DFN-CERT-2024-0022, DFN-CERT:DFN-CERT-2024-0013, DFN-CERT:DFN-CERT-2023-3219, DFN- |

CERT:DFN-CERT-2023-3218, DFN-CERT:DFN-CERT-2023-3210, DFN-CERT:DFN-CERT-2023-3201, DFN-CERT:DFN-CERT-2023-3200, DFN-CERT:DFN-CERT-2023-3195, DFN-CERT:DFN-CERT-2023-3193, DFN-CERT:DFN-CERT-2023-3191, DFN-CERT:DFN-CERT-2023-3185, DFN-CERT:DFN-CERT-2023-3184, DFN-CERT:DFN-CERT-2023-3183, DFN-CERT:DFN-CERT-2023-3182, DFN-CERT:DFN-CERT-2023-3175

## Scanner evidence for A113

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2022-1799, DFN-CERT:DFN-CERT-2023-0201, DFN-CERT:DFN-CERT-2023-0199, DFN-CERT:DFN-CERT-2023-0176, DFN-CERT:DFN-CERT-2023-0153 |

## Scanner evidence for A115

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K19/0477, DFN-CERT:DFN-CERT-2019-1127 |

## Scanner evidence for A116

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2026-1752, CERT-BUND:WID-SEC-2025-1660, CERT-BUND:WID-SEC-2025-1212, CERT-BUND:WID-SEC-2024-1872, CERT-BUND:WID-SEC-2024-1682, CERT-BUND:WID-SEC-2023-0239, CERT-BUND:WID-SEC-2022-0673, CERT-BUND:CB-K22/0045, CERT-BUND:CB-K20/1030, CERT-BUND:CB-K20/0309, CERT-BUND:CB-K20/0041, CERT-BUND:CB-K19/0911, CERT-BUND:CB-K19/0909, CERT-BUND:CB-K19/0615, CERT-BUND:CB-K19/0321, CERT-BUND:CB-K19/0313, CERT-BUND:CB-K19/0054, CERT-BUND:CB-K19/0052, CERT-BUND:CB-K19/0049, CERT-BUND:CB-K19/0048, CERT-BUND:CB-K19/0046, CERT-BUND:CB-K18/1006, DFN-CERT:DFN-CERT-2023-1197, DFN-CERT:DFN-CERT-2023-0245, DFN-CERT:DFN-CERT-2020-2423, DFN-CERT:DFN-CERT-2020-2130, DFN-CERT:DFN-CERT-2020-0630, DFN-CERT:DFN-CERT-2020-0590, DFN-CERT:DFN-CERT-2020-0318, DFN-CERT:DFN-CERT-2019-2158, DFN-CERT:DFN-CERT-2019-1455, DFN-CERT:DFN-CERT-2019-0777, DFN-CERT:DFN-CERT-2019-0772, DFN-CERT:DFN-CERT-2019-0119, DFN-CERT:DFN-CERT-2019-0111, DFN-CERT:DFN-CERT-2018-2103, DFN-CERT:DFN-CERT-2018-1163 |

## Scanner evidence for A117

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2026-1752, CERT-BUND:CB-K17/0195, DFN-CERT:DFN-CERT-2017-0199, DFN-CERT:DFN-CERT-2016-0890 |

## Scanner evidence for A119

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2022-2127, CERT-BUND:CB-K19/0166, CERT-BUND:CB-K17/1252, CERT-BUND:CB-K17/0318, CERT-BUND:CB-K17/0232, CERT-BUND:CB-K17/0182, DFN-CERT:DFN-CERT-2022-2638, DFN-CERT:DFN-CERT-2020-2398, DFN-CERT:DFN-CERT-2020-1078, DFN-CERT:DFN-CERT-2020-0898, DFN-CERT:DFN-CERT-2020-0680, DFN-CERT:DFN-CERT-2019-2283, DFN-CERT:DFN-CERT-2019-1737, DFN-CERT:DFN-CERT-2019-1181, DFN-CERT:DFN-CERT-2019-0804, DFN-CERT:DFN-CERT-2019-0698, DFN-CERT:DFN-CERT-2019-0434, DFN-CERT:DFN-CERT-2019-0368, DFN-CERT:DFN-CERT-2019-0313, DFN-CERT:DFN-CERT-2019-0241, DFN-CERT:DFN-CERT-2019-0212, DFN-CERT:DFN-CERT-2017-1295, DFN-CERT:DFN-CERT-2017-0325, DFN-CERT:DFN-CERT-2017-0234, DFN-CERT:DFN-CERT-2017-0179 |

## Scanner evidence for A120

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2026-1752, CERT-BUND:WID-SEC-2024-1872, CERT-BUND:WID-SEC-2023-1737, CERT-BUND:WID-SEC-2023-0239, CERT-BUND:WID-SEC-2022-1948, CERT-BUND:WID-SEC-2022-1947, CERT-BUND:WID-SEC-2022-0732, CERT-BUND:WID-SEC-2022-0673, CERT-BUND:CB-K22/0045, CERT-BUND:CB-K21/1083, CERT-BUND:CB-K20/1049, CERT-BUND:CB-K20/1030, CERT-BUND:CB-K20/0800, CERT-BUND:CB-K20/0710, CERT-BUND:CB-K20/0324, CERT-BUND:CB-K20/0314, CERT-BUND:CB-K20/0309, CERT-BUND:CB-K20/0106, CERT-BUND:CB-K20/0041, CERT-BUND:CB-K20/0037, CERT-BUND:CB-K20/0034, CERT-BUND:CB-K19/0921, CERT-BUND:CB-K19/0920, CERT-BUND:CB-K19/0916, CERT-BUND:CB-K19/0911, CERT-BUND:CB-K19/0909, CERT-BUND:CB-K19/0619, CERT-BUND:CB-K19/0504, CERT-BUND:CB-K19/0329, DFN-CERT:DFN-CERT-2025-1803, DFN-CERT:DFN-CERT-2024-1997, DFN-CERT:DFN-CERT-2023-2027, DFN-CERT:DFN-CERT-2023-1197, DFN-CERT:DFN-CERT-2023-0481, DFN-CERT:DFN-CERT-2023-0245, DFN-CERT:DFN-CERT-2022-2467, DFN-CERT:DFN-CERT-2021-1536, DFN-CERT:DFN-CERT-2021-1503, DFN-CERT:DFN-CERT-2021-0826, DFN-CERT:DFN-CERT-2020-2423, DFN-CERT:DFN-CERT-2020-2335, DFN-CERT:DFN-CERT-2020-2286, DFN-CERT:DFN-CERT-2020-2130, DFN-CERT:DFN-CERT-2020-1812, DFN-CERT:DFN-CERT-2020-1574, DFN-CERT:DFN-CERT-2020-1537, DFN-CERT:DFN-CERT-2020-1506, DFN-CERT:DFN-CERT-2020-0772, DFN-CERT:DFN-CERT-2020-0769, DFN-CERT:DFN-CERT-2020-0721, DFN-CERT:DFN-CERT-2020-0276, DFN-CERT:DFN-CERT-2020-0102, DFN-CERT:DFN-CERT-2020-0100, DFN-CERT:DFN-CERT-2019-2169, DFN-CERT:DFN-CERT-2019-2158, DFN-CERT:DFN-CERT-2019-2156, DFN-CERT:DFN-CERT-2019-2126, DFN-CERT:DFN-CERT-2019-1861, DFN-CERT:DFN-CERT-2019-1663, DFN-CERT:DFN-CERT-2019-1460, DFN-CERT:DFN-CERT-2019-1182, DFN-CERT:DFN-CERT-2019-1153, DFN-CERT:DFN-CERT-2019-1118, DFN-CERT:DFN-CERT-2019-1033, DFN-CERT:DFN-CERT-2019-0914, DFN-CERT:DFN-CERT-2019-0899, DFN-CERT:DFN-CERT-2019-0805 |

## Scanner evidence for A121

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K20/0857, DFN-CERT:DFN-CERT-2019-2538 |

## Scanner evidence for A122

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K20/0857, CERT-BUND:CB-K20/0324, CERT-BUND:CB-K20/0109, DFN-CERT:DFN-CERT-2020-0550, DFN-CERT:DFN-CERT-2020-0072, DFN-CERT:DFN-CERT-2019-2538, DFN-CERT:DFN-CERT-2019-2533 |

## Scanner evidence for A123

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2025-2723, CERT-BUND:CB-K20/0214, CERT-BUND:CB-K20/0010, DFN-CERT:DFN-CERT-2020-0488, DFN-CERT:DFN-CERT-2020-0089, DFN-CERT:DFN-CERT-2020-0026 |

## Scanner evidence for A124

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2022-2121, CERT-BUND:CB-K20/1199, CERT-BUND:CB-K20/0067, DFN-CERT:DFN-CERT-2022-2638, DFN-CERT:DFN-CERT-2020-2627, DFN-CERT:DFN-CERT-2020-1964, DFN-CERT:DFN-CERT-2020-0485, DFN-CERT:DFN-CERT-2020-0422, DFN- |

| | |
|---|---|
| | CERT:DFN-CERT-2020-0415, DFN-CERT:DFN-CERT-2020-0382, DFN-CERT:DFN-CERT-2020-0342, DFN-CERT:DFN-CERT-2020-0339, DFN-CERT:DFN-CERT-2020-0337, DFN-CERT:DFN-CERT-2020-0139 |

## Scanner evidence for A125

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K20/0130, DFN-CERT:DFN-CERT-2020-2764, DFN-CERT:DFN-CERT-2020-2521, DFN-CERT:DFN-CERT-2020-2311, DFN-CERT:DFN-CERT-2020-1966, DFN-CERT:DFN-CERT-2020-1806, DFN-CERT:DFN-CERT-2020-0626, DFN-CERT:DFN-CERT-2020-0319 |

## Scanner evidence for A126

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K20/1199, CERT-BUND:CB-K20/0336, DFN-CERT:DFN-CERT-2020-1438, DFN-CERT:DFN-CERT-2020-0851, DFN-CERT:DFN-CERT-2020-0751 |

## Scanner evidence for A127

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2022-2117, CERT-BUND:CB-K20/1199, CERT-BUND:CB-K20/0467, DFN-CERT:DFN-CERT-2022-2638, DFN-CERT:DFN-CERT-2020-2627, DFN-CERT:DFN-CERT-2020-2006, DFN-CERT:DFN-CERT-2020-1964, DFN-CERT:DFN-CERT-2020-1438, DFN-CERT:DFN-CERT-2020-1376, DFN-CERT:DFN-CERT-2020-1202, DFN-CERT:DFN-CERT-2020-1019 |

## Scanner evidence for A128

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2022-2115, CERT-BUND:CB-K20/0949, DFN-CERT:DFN-CERT-2022-2639, DFN-CERT:DFN-CERT-2022-2638, DFN-CERT:DFN-CERT-2021-2373, DFN-CERT:DFN-CERT-2021-1645, DFN-CERT:DFN-CERT-2021-0380, DFN-CERT:DFN-CERT-2021-0002, DFN-CERT:DFN-CERT-2020-2187, DFN-CERT:DFN-CERT-2020-2111 |

## Scanner evidence for A129

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2022-1382, CERT-BUND:CB-K20/0825, DFN-CERT:DFN-CERT-2021-0631, DFN-CERT:DFN-CERT-2020-2764, DFN-CERT:DFN-CERT-2020-2656, DFN-CERT:DFN-CERT-2020-2521, DFN-CERT:DFN-CERT-2020-2311, DFN-CERT:DFN-CERT-2020-1966, DFN-CERT:DFN-CERT-2020-1806, DFN-CERT:DFN-CERT-2020-1803 |

## Scanner evidence for A130

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K20/0969, DFN-CERT:DFN-CERT-2020-2526, DFN-CERT:DFN-CERT-2020-2366, DFN-CERT:DFN-CERT-2020-2322, DFN-CERT:DFN-CERT-2020-2220 |

## Scanner evidence for A131

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2023-1737, CERT-BUND:WID-SEC-2022-2114, CERT-BUND:CB-K21/0009, DFN-CERT:DFN-CERT-2024-2707, DFN-CERT:DFN-CERT-2024-1586, DFN-CERT:DFN-CERT-2023-1600, DFN-CERT:DFN-CERT-2022-2639, DFN-CERT:DFN-CERT-2022-2638, DFN- |

CERT:DFN-CERT-2021-2373, DFN-CERT:DFN-CERT-2021-1645, DFN-CERT:DFN-CERT-2021-1509, DFN-CERT:DFN-CERT-2021-1453, DFN-CERT:DFN-CERT-2021-0380, DFN-CERT:DFN-CERT-2021-0013

## Scanner evidence for A132

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2023-1737, CERT-BUND:WID-SEC-2022-2113, CERT-BUND:CB-K21/0124, DFN-CERT:DFN-CERT-2023-1600, DFN-CERT:DFN-CERT-2022-2639, DFN-CERT:DFN-CERT-2022-2638, DFN-CERT:DFN-CERT-2022-0904, DFN-CERT:DFN-CERT-2021-2373, DFN-CERT:DFN-CERT-2021-1645, DFN-CERT:DFN-CERT-2021-1509, DFN-CERT:DFN-CERT-2021-1453, DFN-CERT:DFN-CERT-2021-0556, DFN-CERT:DFN-CERT-2021-0380, DFN-CERT:DFN-CERT-2021-0246 |

## Scanner evidence for A135

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2022-2372, CERT-BUND:WID-SEC-2022-1714, CERT-BUND:CB-K21/1034, DFN-CERT:DFN-CERT-2022-2612, DFN-CERT:DFN-CERT-2022-2269, DFN-CERT:DFN-CERT-2021-2539 |

## Scanner evidence for A136

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K19/0354, DFN-CERT:DFN-CERT-2019-0358, DFN-CERT:DFN-CERT-2018-1764 |

## Scanner evidence for A137

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K15/1518, CERT-BUND:CB-K15/0960, CERT-BUND:CB-K15/0493, CERT-BUND:CB-K15/0079, CERT-BUND:CB-K14/1568, CERT-BUND:CB-K14/1313, CERT-BUND:CB-K14/1110, CERT-BUND:CB-K14/1095, CERT-BUND:CB-K14/1043, CERT-BUND:CB-K14/0969, CERT-BUND:CB-K14/0876, CERT-BUND:CB-K14/0319, DFN-CERT:DFN-CERT-2015-1604, DFN-CERT:DFN-CERT-2015-1008, DFN-CERT:DFN-CERT-2015-0079, DFN-CERT:DFN-CERT-2014-1668, DFN-CERT:DFN-CERT-2014-1166, DFN-CERT:DFN-CERT-2014-1145, DFN-CERT:DFN-CERT-2014-1088, DFN-CERT:DFN-CERT-2014-1019, DFN-CERT:DFN-CERT-2014-0917, DFN-CERT:DFN-CERT-2014-0331 |

## Scanner evidence for A138

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K16/0112, CERT-BUND:CB-K15/1841, CERT-BUND:CB-K15/1517, CERT-BUND:CB-K15/1360, CERT-BUND:CB-K15/1078, CERT-BUND:CB-K15/1011, CERT-BUND:CB-K15/0960, CERT-BUND:CB-K15/0954, CERT-BUND:CB-K15/0806, CERT-BUND:CB-K15/0493, CERT-BUND:CB-K15/0469, CERT-BUND:CB-K15/0079, CERT-BUND:CB-K15/0075, CERT-BUND:CB-K14/1626, CERT-BUND:CB-K14/1592, CERT-BUND:CB-K14/1568, CERT-BUND:CB-K14/1545, CERT-BUND:CB-K14/1095, CERT-BUND:CB-K14/1050, CERT-BUND:CB-K14/1043, CERT-BUND:CB-K14/0969, CERT-BUND:CB-K14/0968, CERT-BUND:CB-K14/0924, CERT-BUND:CB-K14/0883, DFN-CERT:DFN-CERT-2016-0125, DFN-CERT:DFN-CERT-2015-1950, DFN-CERT:DFN-CERT-2015-1608, DFN-CERT:DFN-CERT-2015-1435, DFN-CERT:DFN-CERT-2015-1137, DFN-CERT:DFN-CERT-2015-1069, DFN-CERT:DFN-CERT-2015-1008, DFN-CERT:DFN-CERT-2015-1002, DFN-CERT:DFN-CERT-2015-0842, DFN-CERT:DFN-CERT-2015-0495, DFN-CERT:DFN-CERT-2015-0083, DFN-CERT:DFN-CERT-2015-0079, DFN- |

CERT:DFN-CERT-2014-1727, DFN-CERT:DFN-CERT-2014-1691, DFN-CERT:DFN-CERT-2014-1668, DFN-CERT:DFN-CERT-2014-1633, DFN-CERT:DFN-CERT-2014-1145, DFN-CERT:DFN-CERT-2014-1094, DFN-CERT:DFN-CERT-2014-1088, DFN-CERT:DFN-CERT-2014-1019, DFN-CERT:DFN-CERT-2014-1017, DFN-CERT:DFN-CERT-2014-0967, DFN-CERT:DFN-CERT-2014-0926

## Scanner evidence for A139

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K15/0960, CERT-BUND:CB-K14/1568, CERT-BUND:CB-K14/1095, CERT-BUND:CB-K14/0231, CERT-BUND:CB-K13/1009, CERT-BUND:CB-K13/0600, DFN-CERT:DFN-CERT-2015-1008, DFN-CERT:DFN-CERT-2014-1668, DFN-CERT:DFN-CERT-2014-1145, DFN-CERT:DFN-CERT-2013-2027, DFN-CERT:DFN-CERT-2013-1587, DFN-CERT:DFN-CERT-2013-1503, DFN-CERT:DFN-CERT-2013-1464, DFN-CERT:DFN-CERT-2013-1463, DFN-CERT:DFN-CERT-2013-1456 |

## Scanner evidence for A140

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K15/0960, CERT-BUND:CB-K14/1568, CERT-BUND:CB-K14/1095, CERT-BUND:CB-K14/0231, CERT-BUND:CB-K14/0058, CERT-BUND:CB-K13/1009, CERT-BUND:CB-K13/0600, CERT-BUND:CB-K13/0592, DFN-CERT:DFN-CERT-2015-1008, DFN-CERT:DFN-CERT-2014-1668, DFN-CERT:DFN-CERT-2014-1145, DFN-CERT:DFN-CERT-2014-0049, DFN-CERT:DFN-CERT-2013-2027, DFN-CERT:DFN-CERT-2013-1587, DFN-CERT:DFN-CERT-2013-1585, DFN-CERT:DFN-CERT-2013-1463, DFN-CERT:DFN-CERT-2013-0888 |

## Scanner evidence for A141

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K15/0960, CERT-BUND:CB-K14/0058, CERT-BUND:CB-K13/0600, DFN-CERT:DFN-CERT-2015-1008, DFN-CERT:DFN-CERT-2014-0049, DFN-CERT:DFN-CERT-2013-1587, DFN-CERT:DFN-CERT-2013-1307, DFN-CERT:DFN-CERT-2013-1046, DFN-CERT:DFN-CERT-2013-0944, DFN-CERT:DFN-CERT-2013-0888, DFN-CERT:DFN-CERT-2013-0716, DFN-CERT:DFN-CERT-2013-0661, DFN-CERT:DFN-CERT-2013-0476 |

## Scanner evidence for A142

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K15/1273, CERT-BUND:CB-K15/0960, CERT-BUND:CB-K14/1568, CERT-BUND:CB-K14/1531, DFN-CERT:DFN-CERT-2015-1343, DFN-CERT:DFN-CERT-2015-1008, DFN-CERT:DFN-CERT-2014-1668, DFN-CERT:DFN-CERT-2014-1644, DFN-CERT:DFN-CERT-2013-1307, DFN-CERT:DFN-CERT-2013-0716, DFN-CERT:DFN-CERT-2013-0342, DFN-CERT:DFN-CERT-2013-0270, DFN-CERT:DFN-CERT-2013-0237, DFN-CERT:DFN-CERT-2013-0234, DFN-CERT:DFN-CERT-2013-0040, DFN-CERT:DFN-CERT-2012-2277 |

## Scanner evidence for A143

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2013-0270, DFN-CERT:DFN-CERT-2013-0237, DFN-CERT:DFN-CERT-2012-2277, DFN-CERT:DFN-CERT-2012-1173 |

## Scanner evidence for A144

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K14/1599, DFN-CERT:DFN-CERT-2014-1694, DFN-CERT:DFN-CERT-2013-1307, DFN-CERT:DFN-CERT-2013-0784, DFN-CERT:DFN-CERT-2012-1406, DFN-CERT:DFN-CERT-2012-0731, DFN-CERT:DFN-CERT-2012-0627, DFN-CERT:DFN-CERT-2012-0150, DFN-CERT:DFN-CERT-2011-1725, DFN-CERT:DFN-CERT-2011-1692, DFN-CERT:DFN-CERT-2011-1492, DFN-CERT:DFN-CERT-2011-1379, DFN-CERT:DFN-CERT-2011-0876, DFN-CERT:DFN-CERT-2011-0863, DFN-CERT:DFN-CERT-2011-0848, DFN-CERT:DFN-CERT-2011-0802, DFN-CERT:DFN-CERT-2011-0762, DFN-CERT:DFN-CERT-2011-0761, DFN-CERT:DFN-CERT-2011-0748 |

## Scanner evidence for A145

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2022-2279, CERT-BUND:WID-SEC-2022-1335, CERT-BUND:WID-SEC-2022-1228, CERT-BUND:WID-SEC-2022-0676, CERT-BUND:WID-SEC-2022-0530, CERT-BUND:WID-SEC-2022-0432, CERT-BUND:WID-SEC-2022-0302, CERT-BUND:CB-K21/1173, DFN-CERT:DFN-CERT-2023-2166, DFN-CERT:DFN-CERT-2022-1571, DFN-CERT:DFN-CERT-2022-1469, DFN-CERT:DFN-CERT-2022-0865, DFN-CERT:DFN-CERT-2022-0369, DFN-CERT:DFN-CERT-2022-0348, DFN-CERT:DFN-CERT-2022-0332, DFN-CERT:DFN-CERT-2022-0293, DFN-CERT:DFN-CERT-2021-2566, DFN-CERT:DFN-CERT-2021-2539, DFN-CERT:DFN-CERT-2021-2488, DFN-CERT:DFN-CERT-2021-2424, DFN-CERT:DFN-CERT-2021-2412, DFN-CERT:DFN-CERT-2021-2330 |

## Scanner evidence for A146

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2025-2471, CERT-BUND:WID-SEC-2023-0426, CERT-BUND:WID-SEC-2022-1515, CERT-BUND:WID-SEC-2022-0031, CERT-BUND:CB-K22/0310, CERT-BUND:CB-K22/0127, CERT-BUND:CB-K21/1201, DFN-CERT:DFN-CERT-2022-2776, DFN-CERT:DFN-CERT-2022-2152, DFN-CERT:DFN-CERT-2022-1919, DFN-CERT:DFN-CERT-2022-1885, DFN-CERT:DFN-CERT-2022-0578, DFN-CERT:DFN-CERT-2022-0236, DFN-CERT:DFN-CERT-2021-2638, DFN-CERT:DFN-CERT-2021-2566, DFN-CERT:DFN-CERT-2021-2400 |

## Scanner evidence for A147

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2023-1737, CERT-BUND:WID-SEC-2022-1767, CERT-BUND:WID-SEC-2022-0587, CERT-BUND:WID-SEC-2022-0432, CERT-BUND:WID-SEC-2022-0302, CERT-BUND:CB-K21/1213, DFN-CERT:DFN-CERT-2023-1600, DFN-CERT:DFN-CERT-2022-2869, DFN-CERT:DFN-CERT-2022-2639, DFN-CERT:DFN-CERT-2022-2638, DFN-CERT:DFN-CERT-2022-2598, DFN-CERT:DFN-CERT-2022-2499, DFN-CERT:DFN-CERT-2022-1516, DFN-CERT:DFN-CERT-2022-1493, DFN-CERT:DFN-CERT-2022-0557, DFN-CERT:DFN-CERT-2022-0485, DFN-CERT:DFN-CERT-2022-0455, DFN-CERT:DFN-CERT-2022-0431, DFN-CERT:DFN-CERT-2022-0407, DFN-CERT:DFN-CERT-2022-0110, DFN-CERT:DFN-CERT-2021-2474, DFN-CERT:DFN-CERT-2021-2436 |

## Scanner evidence for A148

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2022-0465, CERT-BUND:CB-K22/0027, DFN-CERT:DFN-CERT-2022-1032, DFN-CERT:DFN-CERT-2022-0264, DFN-CERT:DFN-CERT-2022-0242 |

## Scanner evidence for A149

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2022-1335, CERT-BUND:WID-SEC-2022-1228, CERT-BUND:WID-SEC-2022-0466, CERT-BUND:WID-SEC-2022-0432, CERT-BUND:WID-SEC-2022-0302, CERT-BUND:CB-K22/0128, DFN-CERT:DFN-CERT-2022-0557, DFN-CERT:DFN-CERT-2022-0348, DFN-CERT:DFN-CERT-2022-0332, DFN-CERT:DFN-CERT-2022-0264, DFN-CERT:DFN-CERT-2022-0242, DFN-CERT:DFN-CERT-2022-0239, DFN-CERT:DFN-CERT-2022-0232, DFN-CERT:DFN-CERT-2022-0228 |

## Scanner evidence for A150

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2022-0466, CERT-BUND:CB-K22/0128, DFN-CERT:DFN-CERT-2022-1032, DFN-CERT:DFN-CERT-2022-0264, DFN-CERT:DFN-CERT-2022-0242, DFN-CERT:DFN-CERT-2022-0228 |

## Scanner evidence for A151

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2023-1737, CERT-BUND:WID-SEC-2022-1767, CERT-BUND:WID-SEC-2022-1335, CERT-BUND:WID-SEC-2022-1228, CERT-BUND:WID-SEC-2022-0280, CERT-BUND:CB-K22/0201, DFN-CERT:DFN-CERT-2024-1062, DFN-CERT:DFN-CERT-2023-1600, DFN-CERT:DFN-CERT-2022-2639, DFN-CERT:DFN-CERT-2022-2598, DFN-CERT:DFN-CERT-2022-2500, DFN-CERT:DFN-CERT-2022-2499, DFN-CERT:DFN-CERT-2022-1605, DFN-CERT:DFN-CERT-2022-0557, DFN-CERT:DFN-CERT-2022-0407, DFN-CERT:DFN-CERT-2022-0365 |

## Scanner evidence for A152

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2023-3005, CERT-BUND:CB-K22/0304, DFN-CERT:DFN-CERT-2023-0379, DFN-CERT:DFN-CERT-2022-0570 |

## Scanner evidence for A153

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2023-1737, CERT-BUND:WID-SEC-2022-0255, CERT-BUND:CB-K22/0700, DFN-CERT:DFN-CERT-2023-1600, DFN-CERT:DFN-CERT-2022-2869, DFN-CERT:DFN-CERT-2022-2639, DFN-CERT:DFN-CERT-2022-2638, DFN-CERT:DFN-CERT-2022-2598, DFN-CERT:DFN-CERT-2022-2500, DFN-CERT:DFN-CERT-2022-2323, DFN-CERT:DFN-CERT-2022-1881, DFN-CERT:DFN-CERT-2022-1552, DFN-CERT:DFN-CERT-2022-1516, DFN-CERT:DFN-CERT-2022-1493, DFN-CERT:DFN-CERT-2022-1473, DFN-CERT:DFN-CERT-2022-1288 |

## Scanner evidence for A154

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2023-1021, CERT-BUND:WID-SEC-2023-0561, CERT-BUND:WID-SEC-2023-0138, CERT-BUND:WID-SEC-2022-1934, CERT-BUND:WID-SEC-2022-1816, DFN-CERT:DFN-CERT-2026-0215, DFN-CERT:DFN-CERT-2023-0552, DFN-CERT:DFN-CERT-2023-0422, DFN-CERT:DFN-CERT-2023-0028, DFN-CERT:DFN-CERT-2022-2869, DFN-CERT:DFN-CERT-2022-2793, DFN-CERT:DFN-CERT-2022-2715, DFN-CERT:DFN-CERT-2022-2639, DFN-CERT:DFN-CERT-2022-2638, DFN-CERT:DFN-CERT-2022-2598, DFN-CERT:DFN-CERT-2022-2535, DFN-CERT:DFN-CERT-2022-2523, DFN-CERT:DFN-CERT-2022-2420, DFN-CERT:DFN-CERT-2022-2380 |

## Scanner evidence for A155

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2023-0035, DFN-CERT:DFN-CERT-2023-0435, DFN-CERT:DFN-CERT-2023-0422, DFN-CERT:DFN-CERT-2023-0071, DFN-CERT:DFN-CERT-2023-0034 |

## Scanner evidence for A156

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2023-2917, CERT-BUND:WID-SEC-2023-2680, CERT-BUND:WID-SEC-2023-1506, DFN-CERT:DFN-CERT-2024-3330, DFN-CERT:DFN-CERT-2023-2570, DFN-CERT:DFN-CERT-2023-2542, DFN-CERT:DFN-CERT-2023-1328 |

## Scanner evidence for A161

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2012-0730, DFN-CERT:DFN-CERT-2012-0727, DFN-CERT:DFN-CERT-2012-0721, DFN-CERT:DFN-CERT-2012-0462, DFN-CERT:DFN-CERT-2012-0444, DFN-CERT:DFN-CERT-2012-0390, DFN-CERT:DFN-CERT-2012-0356 |

## Scanner evidence for A162

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2013-0359, DFN-CERT:DFN-CERT-2013-0351, DFN-CERT:DFN-CERT-2012-1172, DFN-CERT:DFN-CERT-2012-1111, DFN-CERT:DFN-CERT-2012-0986, DFN-CERT:DFN-CERT-2012-0950, DFN-CERT:DFN-CERT-2012-0929, DFN-CERT:DFN-CERT-2012-0850, DFN-CERT:DFN-CERT-2012-0764, DFN-CERT:DFN-CERT-2012-0748, DFN-CERT:DFN-CERT-2012-0730, DFN-CERT:DFN-CERT-2012-0727, DFN-CERT:DFN-CERT-2012-0726, DFN-CERT:DFN-CERT-2012-0721, DFN-CERT:DFN-CERT-2012-0720, DFN-CERT:DFN-CERT-2012-0719, DFN-CERT:DFN-CERT-2012-0718, DFN-CERT:DFN-CERT-2012-0713, DFN-CERT:DFN-CERT-2012-0666, DFN-CERT:DFN-CERT-2012-0665, DFN-CERT:DFN-CERT-2012-0657 |

## Scanner evidence for A163

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K14/0986, CERT-BUND:CB-K14/0696, CERT-BUND:CB-K13/0714, CERT-BUND:CB-K13/0704, DFN-CERT:DFN-CERT-2014-1026, DFN-CERT:DFN-CERT-2014-0726, DFN-CERT:DFN-CERT-2013-1714, DFN-CERT:DFN-CERT-2013-1700, DFN-CERT:DFN-CERT-2013-1500, DFN-CERT:DFN-CERT-2013-1488, DFN-CERT:DFN-CERT-2013-1462, DFN-CERT:DFN-CERT-2013-1454 |

## Scanner evidence for A164

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2026-3111, CERT-BUND:CB-K16/0718, CERT-BUND:CB-K16/0596, CERT-BUND:CB-K16/0589, CERT-BUND:CB-K16/0572, CERT-BUND:CB-K15/1849, DFN-CERT:DFN-CERT-2016-0772, DFN-CERT:DFN-CERT-2016-0648, DFN-CERT:DFN-CERT-2016-0639, DFN-CERT:DFN-CERT-2016-0620, DFN-CERT:DFN-CERT-2015-1948 |

## Scanner evidence for A165

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2024-0867, DFN-CERT:DFN-CERT-2025-1211, DFN-CERT:DFN-CERT-2024-3330, DFN-CERT:DFN-CERT-2024-3329, DFN-CERT:DFN-CERT-2024-1574, DFN-CERT:DFN-CERT-2024-1192, DFN-CERT:DFN-CERT-2024-1132, DFN-CERT:DFN-CERT-2024-1115, DFN-CERT:DFN-CERT-2024-0993, DFN-CERT:DFN-CERT-2024-0962 |

## Scanner evidence for A166

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2024-3196, CERT-BUND:WID-SEC-2024-3195, CERT-BUND:WID-SEC-2024-1320, DFN-CERT:DFN-CERT-2025-1211, DFN-CERT:DFN-CERT-2024-3330, DFN-CERT:DFN-CERT-2024-3329, DFN-CERT:DFN-CERT-2024-2707, DFN-CERT:DFN-CERT-2024-1853, DFN-CERT:DFN-CERT-2024-1586, DFN-CERT:DFN-CERT-2024-1574, DFN-CERT:DFN-CERT-2024-1563, DFN-CERT:DFN-CERT-2024-1476 |

## Scanner evidence for A167

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2024-3519, DFN-CERT:DFN-CERT-2026-0499, DFN-CERT:DFN-CERT-2025-1211, DFN-CERT:DFN-CERT-2025-1082, DFN-CERT:DFN-CERT-2025-0179, DFN-CERT:DFN-CERT-2024-3200, DFN-CERT:DFN-CERT-2024-3172, DFN-CERT:DFN-CERT-2024-3108 |

## Scanner evidence for A168

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2025-1439, CERT-BUND:WID-SEC-2025-0372, DFN-CERT:DFN-CERT-2025-0371 |

## Scanner evidence for A169

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2025-0566, DFN-CERT:DFN-CERT-2026-0499, DFN-CERT:DFN-CERT-2025-1939, DFN-CERT:DFN-CERT-2025-1082, DFN-CERT:DFN-CERT-2025-0665 |

## Scanner evidence for A170

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2026-1118, CERT-BUND:WID-SEC-2025-1439, CERT-BUND:WID-SEC-2025-0986, DFN-CERT:DFN-CERT-2025-1179 |

## Scanner evidence for A171

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2026-2437, CERT-BUND:WID-SEC-2025-1460, DFN-CERT:DFN-CERT-2026-0499, DFN-CERT:DFN-CERT-2026-0315, DFN-CERT:DFN-CERT-2025-1785 |

## Scanner evidence for A172

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2026-0351, CERT-BUND:WID-SEC-2025-2140, CERT-BUND:WID-SEC-2025-1842, DFN-CERT:DFN-CERT-2025-2667, DFN-CERT:DFN-CERT-2025-2360, DFN-CERT:DFN-CERT-2025-2233 |

## Scanner evidence for A173

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2026-1032, CERT-BUND:WID-SEC-2025-0810, CERT-BUND:WID-SEC-2025-0168, CERT-BUND:WID-SEC-2025-0144, CERT-BUND:WID-SEC-2025-0139, CERT-BUND:WID-SEC-2024-3377, CERT-BUND:WID-SEC-2024-3320, CERT-BUND:WID-SEC-2024-3198, CERT-BUND:WID-SEC-2024-3195, CERT-BUND:WID-SEC-2024-1913, CERT-BUND:WID-SEC-2024-1781, CERT-BUND:WID-SEC-2024-1701, CERT-BUND:WID-SEC-2024-1656, CERT-BUND:WID-SEC-2024-1655, CERT-BUND:WID-SEC-2024-1643, CERT-BUND:WID-SEC-2024-1642, CERT-BUND:WID-SEC-2024-1639, CERT-BUND:WID-SEC-2024-1637, CERT-BUND:WID-SEC-2024-1630, CERT-BUND:WID-SEC-2024-1474, CERT-BUND:WID-SEC-2024-1248, CERT-BUND:WID-SEC-2024-1228, CERT-BUND:WID-SEC-2024-1186, CERT-BUND:WID-SEC-2024-1082, CERT-BUND:WID-SEC-2024-0899, CERT-BUND:WID-SEC-2024-0892, CERT-BUND:WID-SEC-2024-0889, CERT-BUND:WID-SEC-2024-0885, CERT-BUND:WID-SEC-2024-0874, CERT-BUND:WID-SEC-2024-0869, CERT-BUND:WID-SEC-2024-0578, CERT-BUND:WID-SEC-2024-0564, CERT-BUND:WID-SEC-2024-0523, CERT-BUND:WID-SEC-2023-3174, DFN-CERT:DFN-CERT-2026-0097, DFN-CERT:DFN-CERT-2025-3629, DFN-CERT:DFN-CERT-2025-3272, DFN-CERT:DFN-CERT-2025-2058, DFN-CERT:DFN-CERT-2025-2037, DFN-CERT:DFN-CERT-2025-1447, DFN-CERT:DFN-CERT-2025-1177, DFN-CERT:DFN-CERT-2025-1025, DFN-CERT:DFN-CERT-2025-0660, DFN-CERT:DFN-CERT-2025-0502, DFN-CERT:DFN-CERT-2025-0294, DFN-CERT:DFN-CERT-2025-0173, DFN-CERT:DFN-CERT-2025-0165, DFN-CERT:DFN-CERT-2025-0024, DFN-CERT:DFN-CERT-2024-3171, DFN-CERT:DFN-CERT-2024-2818, DFN-CERT:DFN-CERT-2024-2759, DFN-CERT:DFN-CERT-2024-2741, DFN-CERT:DFN-CERT-2024-2602, DFN-CERT:DFN-CERT-2024-2573, DFN-CERT:DFN-CERT-2024-2392, DFN-CERT:DFN-CERT-2024-2210, DFN-CERT:DFN-CERT-2024-2209, DFN-CERT:DFN-CERT-2024-2194, DFN-CERT:DFN-CERT-2024-2169, DFN-CERT:DFN-CERT-2024-2048, DFN-CERT:DFN-CERT-2024-2030, DFN-CERT:DFN-CERT-2024-2028, DFN-CERT:DFN-CERT-2024-1930, DFN-CERT:DFN-CERT-2024-1895, DFN-CERT:DFN-CERT-2024-1869, DFN-CERT:DFN-CERT-2024-1868, DFN-CERT:DFN-CERT-2024-1865, DFN-CERT:DFN-CERT-2024-1862, DFN-CERT:DFN-CERT-2024-1854, DFN-CERT:DFN-CERT-2024-1846, DFN-CERT:DFN-CERT-2024-1817, DFN-CERT:DFN-CERT-2024-1715, DFN-CERT:DFN-CERT-2024-1698, DFN-CERT:DFN-CERT-2024-1688, DFN-CERT:DFN-CERT-2024-1655, DFN-CERT:DFN-CERT-2024-1600, DFN-CERT:DFN-CERT-2024-1443, DFN-CERT:DFN-CERT-2024-1442, DFN-CERT:DFN-CERT-2024-1413, DFN-CERT:DFN-CERT-2024-1382, DFN-CERT:DFN-CERT-2024-1380, DFN-CERT:DFN-CERT-2024-1373, DFN-CERT:DFN-CERT-2024-1260, DFN-CERT:DFN-CERT-2024-1259, DFN-CERT:DFN-CERT-2024-1108, DFN-CERT:DFN-CERT-2024-1061, DFN-CERT:DFN-CERT-2024-1029, DFN-CERT:DFN-CERT-2024-1003, DFN-CERT:DFN-CERT-2024-1000, DFN-CERT:DFN-CERT-2024-0896, DFN-CERT:DFN-CERT-2024-0779, DFN-CERT:DFN-CERT-2024-0762, DFN-CERT:DFN-CERT-2024-0744, DFN-CERT:DFN-CERT-2024-0698, DFN-CERT:DFN-CERT-2024-0633, DFN-CERT:DFN-CERT-2024-0619, DFN-CERT:DFN-CERT-2024-0618, DFN-CERT:DFN-CERT-2024-0616, DFN-CERT:DFN-CERT-2024-0597, DFN-CERT:DFN-CERT-2024-0545, DFN-CERT:DFN-CERT-2024-0526, DFN-CERT:DFN-CERT-2024-0491, DFN-CERT:DFN-CERT-2024-0451, DFN-CERT:DFN-CERT-2024-0440, DFN-CERT:DFN-CERT-2024-0420, DFN-CERT:DFN-CERT-2024-0388, DFN-CERT:DFN-CERT-2024-0343, DFN-CERT:DFN-CERT-2024-0306, DFN-CERT:DFN-CERT-2024-0299, DFN-CERT:DFN-CERT-2024-0285, DFN-CERT:DFN-CERT-2024-0267, DFN-CERT:DFN-CERT-2024-0251, DFN-CERT:DFN-CERT-2024-0215, DFN-CERT:DFN-CERT-2024-0211, DFN-CERT:DFN-CERT-2024-0164, DFN-CERT:DFN-CERT-2024-0154, DFN-CERT:DFN-CERT-2024-0101, DFN-CERT:DFN-CERT-2024-0092, DFN-CERT:DFN-CERT-2024-0088, DFN-CERT:DFN-CERT-2024-0067, DFN-CERT:DFN-CERT-2024-0063, DFN-CERT:DFN-CERT-2024-0062, DFN-CERT:DFN- |

CERT-2024-0024, DFN-CERT:DFN-CERT-2024-0013, DFN-CERT:DFN-CERT-2023-3219, DFN-CERT:DFN-CERT-2023-3218, DFN-CERT:DFN-CERT-2023-3210, DFN-CERT:DFN-CERT-2023-3201, DFN-CERT:DFN-CERT-2023-3200, DFN-CERT:DFN-CERT-2023-3195, DFN-CERT:DFN-CERT-2023-3193, DFN-CERT:DFN-CERT-2023-3191, DFN-CERT:DFN-CERT-2023-3185, DFN-CERT:DFN-CERT-2023-3184, DFN-CERT:DFN-CERT-2023-3183, DFN-CERT:DFN-CERT-2023-3182, DFN-CERT:DFN-CERT-2023-3175

## Scanner evidence for A174

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2024-3564, DFN-CERT:DFN-CERT-2025-0772, DFN-CERT:DFN-CERT-2025-0509, DFN-CERT:DFN-CERT-2024-3291, DFN-CERT:DFN-CERT-2024-3171 |

## Scanner evidence for A175

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2025-0295, DFN-CERT:DFN-CERT-2025-1316, DFN-CERT:DFN-CERT-2025-0772, DFN-CERT:DFN-CERT-2025-0564, DFN-CERT:DFN-CERT-2025-0372 |

## Scanner evidence for A176

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2026-2858, CERT-BUND:WID-SEC-2026-0349, CERT-BUND:WID-SEC-2025-2600, DFN-CERT:DFN-CERT-2026-4167, DFN-CERT:DFN-CERT-2026-0744, DFN-CERT:DFN-CERT-2025-3194 |

## Scanner evidence for A177

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2026-1730, DFN-CERT:DFN-CERT-2026-0791, DFN-CERT:DFN-CERT-2026-0651, DFN-CERT:DFN-CERT-2026-0607, DFN-CERT:DFN-CERT-2026-0499, DFN-CERT:DFN-CERT-2026-0315, DFN-CERT:DFN-CERT-2026-0287, DFN-CERT:DFN-CERT-2026-0262, DFN-CERT:DFN-CERT-2025-3544 |

## Scanner evidence for A178

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2023-2917, CERT-BUND:WID-SEC-2023-2679, CERT-BUND:WID-SEC-2023-1970, DFN-CERT:DFN-CERT-2024-3330, DFN-CERT:DFN-CERT-2024-2681, DFN-CERT:DFN-CERT-2024-0993, DFN-CERT:DFN-CERT-2023-2570, DFN-CERT:DFN-CERT-2023-2542, DFN-CERT:DFN-CERT-2023-1775 |

## Scanner evidence for A181

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2009-1129 |

## Scanner evidence for A183

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2010-1665, DFN-CERT:DFN-CERT-2010-1647, DFN-CERT:DFN-CERT-2009-1725, DFN-CERT:DFN-CERT-2009-1507, DFN-CERT:DFN-CERT-2009-1225 |

## Scanner evidence for A184

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2011-0700, DFN-CERT:DFN-CERT-2010-1665, DFN-CERT:DFN-CERT-2010-1647, DFN-CERT:DFN-CERT-2009-1725, DFN-CERT:DFN-CERT-2009-1602, DFN-CERT:DFN-CERT-2009-1507, DFN-CERT:DFN-CERT-2009-1225, DFN-CERT:DFN-CERT-2009-1101 |

## Scanner evidence for A185

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2010-1227, DFN-CERT:DFN-CERT-2010-0802, DFN-CERT:DFN-CERT-2010-0263, DFN-CERT:DFN-CERT-2010-0075, DFN-CERT:DFN-CERT-2010-0074, DFN-CERT:DFN-CERT-2009-1726, DFN-CERT:DFN-CERT-2009-1665, DFN-CERT:DFN-CERT-2009-1663, DFN-CERT:DFN-CERT-2009-1652 |

## Scanner evidence for A186

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2012-1278, DFN-CERT:DFN-CERT-2010-0263, DFN-CERT:DFN-CERT-2010-0143, DFN-CERT:DFN-CERT-2010-0140, DFN-CERT:DFN-CERT-2010-0060, DFN-CERT:DFN-CERT-2010-0011, DFN-CERT:DFN-CERT-2009-1726, DFN-CERT:DFN-CERT-2009-1720, DFN-CERT:DFN-CERT-2009-1629, DFN-CERT:DFN-CERT-2009-1490, DFN-CERT:DFN-CERT-2009-1487 |

## Scanner evidence for A187

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2010-1321, DFN-CERT:DFN-CERT-2010-1247 |

## Scanner evidence for A188

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2011-0642, DFN-CERT:DFN-CERT-2011-0402, DFN-CERT:DFN-CERT-2011-0148, DFN-CERT:DFN-CERT-2011-0147, DFN-CERT:DFN-CERT-2011-0013, DFN-CERT:DFN-CERT-2011-0012, DFN-CERT:DFN-CERT-2011-0011, DFN-CERT:DFN-CERT-2010-1664, DFN-CERT:DFN-CERT-2010-1471 |

## Scanner evidence for A189

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2011-0515 |

## Scanner evidence for A190

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2011-0368, DFN-CERT:DFN-CERT-2010-1551, DFN-CERT:DFN-CERT-2010-1550, DFN-CERT:DFN-CERT-2010-1539 |

## Scanner evidence for A191

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2023-1284, DFN-CERT:DFN-CERT-2013-1538 |

## Scanner evidence for A192

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K14/1480, DFN-CERT:DFN-CERT-2014-1566 |

## Scanner evidence for A193

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K15/0493, CERT-BUND:CB-K14/1359, CERT-BUND:CB-K14/0972, CERT-BUND:CB-K13/1092, CERT-BUND:CB-K13/1040, DFN-CERT:DFN-CERT-2014-1434, DFN-CERT:DFN-CERT-2014-1014, DFN-CERT:DFN-CERT-2013-2127, DFN-CERT:DFN-CERT-2013-2066 |

## Scanner evidence for A194

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2023-1283, CERT-BUND:CB-K17/1176, CERT-BUND:CB-K14/0834, CERT-BUND:CB-K14/0231, CERT-BUND:CB-K13/1092, CERT-BUND:CB-K13/1040, CERT-BUND:CB-K13/1037, CERT-BUND:CB-K13/1036, DFN-CERT:DFN-CERT-2017-1209, DFN-CERT:DFN-CERT-2014-0870, DFN-CERT:DFN-CERT-2013-2127, DFN-CERT:DFN-CERT-2013-2066, DFN-CERT:DFN-CERT-2013-2065, DFN-CERT:DFN-CERT-2013-2064 |

## Scanner evidence for A195

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K15/0493, CERT-BUND:CB-K15/0454, CERT-BUND:CB-K14/1359, CERT-BUND:CB-K14/1215, CERT-BUND:CB-K14/1214, CERT-BUND:CB-K14/1052, CERT-BUND:CB-K14/1051, CERT-BUND:CB-K14/0904, CERT-BUND:CB-K14/0834, CERT-BUND:CB-K14/0830, CERT-BUND:CB-K14/0829, CERT-BUND:CB-K14/0738, DFN-CERT:DFN-CERT-2016-0876, DFN-CERT:DFN-CERT-2015-0473, DFN-CERT:DFN-CERT-2014-1434, DFN-CERT:DFN-CERT-2014-1280, DFN-CERT:DFN-CERT-2014-1279, DFN-CERT:DFN-CERT-2014-1098, DFN-CERT:DFN-CERT-2014-1095, DFN-CERT:DFN-CERT-2014-0936, DFN-CERT:DFN-CERT-2014-0870, DFN-CERT:DFN-CERT-2014-0868, DFN-CERT:DFN-CERT-2014-0867, DFN-CERT:DFN-CERT-2014-0769 |

## Scanner evidence for A196

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K15/1704, CERT-BUND:CB-K15/0493, CERT-BUND:CB-K14/1359, CERT-BUND:CB-K14/1267, CERT-BUND:CB-K14/1174, CERT-BUND:CB-K14/1130, CERT-BUND:CB-K14/0973, CERT-BUND:CB-K14/0972, CERT-BUND:CB-K14/0830, CERT-BUND:CB-K14/0818, CERT-BUND:CB-K14/0776, CERT-BUND:CB-K14/0738, CERT-BUND:CB-K14/0660, CERT-BUND:CB-K14/0659, DFN-CERT:DFN-CERT-2015-1799, DFN-CERT:DFN-CERT-2014-1434, DFN-CERT:DFN-CERT-2014-1333, DFN-CERT:DFN-CERT-2014-1181, DFN-CERT:DFN-CERT-2014-1014, DFN-CERT:DFN-CERT-2014-1013, DFN-CERT:DFN-CERT-2014-0868, DFN-CERT:DFN-CERT-2014-0857, DFN-CERT:DFN-CERT-2014-0816, DFN-CERT:DFN-CERT-2014-0769, DFN-CERT:DFN-CERT-2014-0685, DFN-CERT:DFN-CERT-2014-0684 |

## Scanner evidence for A197

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2026-0180, CERT-BUND:CB-K18/0799, CERT-BUND:CB-K16/1289, CERT-BUND:CB-K16/1096, CERT-BUND:CB-K15/1751, CERT-BUND:CB-K15/1266, CERT-BUND:CB-K15/0850, CERT-BUND:CB-K15/0764, CERT-BUND:CB-K15/0720, CERT-BUND:CB-K15/0548, CERT-BUND:CB-K15/0526, CERT-BUND:CB-K15/0509, CERT-BUND:CB-K15/0493, CERT-BUND:CB-K15/0384, CERT-BUND:CB-K15/0365, CERT-BUND:CB-K15/0364, CERT-BUND:CB-K15/0302, CERT-BUND:CB-K15/0192, CERT-BUND:CB-K15/0016, DFN-CERT:DFN-CERT-2018-1408, DFN-CERT:DFN-CERT-2016-1372, DFN-CERT:DFN-CERT-2016-1164, DFN-CERT:DFN-CERT-2016-0388, DFN-CERT:DFN-CERT-2015-1853, DFN-CERT:DFN-CERT-2015-1332, DFN-CERT:DFN-CERT-2015-0884, DFN-CERT:DFN-CERT-2015-0800, DFN-CERT:DFN-CERT-2015-0758, DFN-CERT:DFN-CERT-2015-0567, DFN-CERT:DFN-CERT-2015-0544, DFN-CERT:DFN-CERT-2015-0530, DFN-CERT:DFN-CERT-2015-0396, DFN-CERT:DFN-CERT-2015-0375, DFN-CERT:DFN-CERT-2015-0374, DFN-CERT:DFN-CERT-2015-0305, DFN-CERT:DFN-CERT-2015-0199, DFN-CERT:DFN-CERT-2015-0021 |

## Scanner evidence for A198

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2023-0069, CERT-BUND:CB-K17/1176, CERT-BUND:CB-K16/0944, CERT-BUND:CB-K15/1437, CERT-BUND:CB-K15/0966, CERT-BUND:CB-K15/0854, CERT-BUND:CB-K15/0806, CERT-BUND:CB-K15/0769, CERT-BUND:CB-K15/0757, CERT-BUND:CB-K15/0665, CERT-BUND:CB-K15/0482, CERT-BUND:CB-K15/0454, CERT-BUND:CB-K15/0420, DFN-CERT:DFN-CERT-2023-0071, DFN-CERT:DFN-CERT-2017-1209, DFN-CERT:DFN-CERT-2016-1004, DFN-CERT:DFN-CERT-2016-0876, DFN-CERT:DFN-CERT-2015-1514, DFN-CERT:DFN-CERT-2015-1017, DFN-CERT:DFN-CERT-2015-0900, DFN-CERT:DFN-CERT-2015-0842, DFN-CERT:DFN-CERT-2015-0809, DFN-CERT:DFN-CERT-2015-0794, DFN-CERT:DFN-CERT-2015-0697, DFN-CERT:DFN-CERT-2015-0505, DFN-CERT:DFN-CERT-2015-0473, DFN-CERT:DFN-CERT-2015-0442 |

## Scanner evidence for A199

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K15/1437, CERT-BUND:CB-K15/0757, CERT-BUND:CB-K15/0215, CERT-BUND:CB-K15/0207, CERT-BUND:CB-K15/0095, DFN-CERT:DFN-CERT-2015-1514, DFN-CERT:DFN-CERT-2015-0794, DFN-CERT:DFN-CERT-2015-0223, DFN-CERT:DFN-CERT-2015-0212, DFN-CERT:DFN-CERT-2015-0093 |

## Scanner evidence for A200

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K15/1360, CERT-BUND:CB-K15/1188, CERT-BUND:CB-K15/1051, CERT-BUND:CB-K15/0273, CERT-BUND:CB-K14/1592, DFN-CERT:DFN-CERT-2015-1435, DFN-CERT:DFN-CERT-2015-1252, DFN-CERT:DFN-CERT-2015-1087, DFN-CERT:DFN-CERT-2015-0285, DFN-CERT:DFN-CERT-2014-1691 |

## Scanner evidence for A201

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2023-1281, CERT-BUND:WID-SEC-2023-0069, CERT-BUND:CB-K16/0944, CERT-BUND:CB-K15/1437, CERT-BUND:CB-K15/1188, CERT-BUND:CB-K15/1031, CERT-BUND:CB-K15/0966, CERT-BUND:CB-K15/0942, CERT-BUND:CB-K15/0854, CERT-BUND:CB-K15/0809, CERT-BUND:CB-K15/0806, CERT-BUND:CB-K15/0769, CERT-BUND:CB-K15/0757, |

CERT-BUND:CB-K15/0665, CERT-BUND:CB-K15/0561, CERT-BUND:CB-K15/0482, CERT-BUND:CB-K15/0377, CERT-BUND:CB-K15/0375, CERT-BUND:CB-K15/0372, DFN-CERT:DFN-CERT-2016-1004, DFN-CERT:DFN-CERT-2015-1514, DFN-CERT:DFN-CERT-2015-1252, DFN-CERT:DFN-CERT-2015-1083, DFN-CERT:DFN-CERT-2015-1017, DFN-CERT:DFN-CERT-2015-0989, DFN-CERT:DFN-CERT-2015-0900, DFN-CERT:DFN-CERT-2015-0854, DFN-CERT:DFN-CERT-2015-0842, DFN-CERT:DFN-CERT-2015-0809, DFN-CERT:DFN-CERT-2015-0794, DFN-CERT:DFN-CERT-2015-0697, DFN-CERT:DFN-CERT-2015-0583, DFN-CERT:DFN-CERT-2015-0505, DFN-CERT:DFN-CERT-2015-0387, DFN-CERT:DFN-CERT-2015-0383, DFN-CERT:DFN-CERT-2015-0382

## Scanner evidence for A202

The action above covers the following detailed scanner evidence.

Vendor references

CERT-BUND:CB-K16/0944, CERT-BUND:CB-K15/1437, CERT-BUND:CB-K15/1188, CERT-BUND:CB-K15/1158, CERT-BUND:CB-K15/1129, CERT-BUND:CB-K15/1031, CERT-BUND:CB-K15/0966, CERT-BUND:CB-K15/0942, CERT-BUND:CB-K15/0936, CERT-BUND:CB-K15/0880, CERT-BUND:CB-K15/0854, CERT-BUND:CB-K15/0806, CERT-BUND:CB-K15/0769, CERT-BUND:CB-K15/0763, CERT-BUND:CB-K15/0757, CERT-BUND:CB-K15/0665, CERT-BUND:CB-K15/0648, CERT-BUND:CB-K15/0561, CERT-BUND:CB-K15/0552, CERT-BUND:CB-K15/0207, DFN-CERT:DFN-CERT-2023-0071, DFN-CERT:DFN-CERT-2016-1004, DFN-CERT:DFN-CERT-2015-1514, DFN-CERT:DFN-CERT-2015-1252, DFN-CERT:DFN-CERT-2015-1217, DFN-CERT:DFN-CERT-2015-1188, DFN-CERT:DFN-CERT-2015-1083, DFN-CERT:DFN-CERT-2015-1017, DFN-CERT:DFN-CERT-2015-0989, DFN-CERT:DFN-CERT-2015-0983, DFN-CERT:DFN-CERT-2015-0926, DFN-CERT:DFN-CERT-2015-0900, DFN-CERT:DFN-CERT-2015-0842, DFN-CERT:DFN-CERT-2015-0809, DFN-CERT:DFN-CERT-2015-0803, DFN-CERT:DFN-CERT-2015-0794, DFN-CERT:DFN-CERT-2015-0697, DFN-CERT:DFN-CERT-2015-0677, DFN-CERT:DFN-CERT-2015-0583, DFN-CERT:DFN-CERT-2015-0579, DFN-CERT:DFN-CERT-2015-0212

## Scanner evidence for A203

The action above covers the following detailed scanner evidence.

Vendor references

CERT-BUND:CB-K15/1437, CERT-BUND:CB-K15/1188, CERT-BUND:CB-K15/0880, CERT-BUND:CB-K15/0854, CERT-BUND:CB-K15/0665, CERT-BUND:CB-K15/0648, CERT-BUND:CB-K15/0561, DFN-CERT:DFN-CERT-2015-1514, DFN-CERT:DFN-CERT-2015-1252, DFN-CERT:DFN-CERT-2015-0926, DFN-CERT:DFN-CERT-2015-0900, DFN-CERT:DFN-CERT-2015-0697, DFN-CERT:DFN-CERT-2015-0677, DFN-CERT:DFN-CERT-2015-0583

## Scanner evidence for A204

The action above covers the following detailed scanner evidence.

Vendor references

CERT-BUND:CB-K17/2123, CERT-BUND:CB-K16/0944, CERT-BUND:CB-K15/1188, CERT-BUND:CB-K15/1082, CERT-BUND:CB-K15/1031, CERT-BUND:CB-K15/0973, CERT-BUND:CB-K15/0966, CERT-BUND:CB-K15/0942, CERT-BUND:CB-K15/0923, CERT-BUND:CB-K15/0880, CERT-BUND:CB-K15/0854, CERT-BUND:CB-K15/0769, CERT-BUND:CB-K15/0763, CERT-BUND:CB-K15/0759, CERT-BUND:CB-K15/0703, DFN-CERT:DFN-CERT-2017-2219, DFN-CERT:DFN-CERT-2016-1004, DFN-CERT:DFN-CERT-2015-1252, DFN-CERT:DFN-CERT-2015-1139, DFN-CERT:DFN-CERT-2015-1083, DFN-CERT:DFN-CERT-2015-1021, DFN-CERT:DFN-CERT-2015-1017, DFN-CERT:DFN-CERT-2015-0989, DFN-CERT:DFN-CERT-2015-0973, DFN-CERT:DFN-CERT-2015-0926, DFN-CERT:DFN-CERT-2015-0900, DFN-CERT:DFN-CERT-2015-0809, DFN-CERT:DFN-CERT-2015-0803, DFN-CERT:DFN-CERT-2015-0797, DFN-CERT:DFN-CERT-2015-0732

## Scanner evidence for A205

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2023-0069, CERT-BUND:CB-K16/0944, CERT-BUND:CB-K15/1561, CERT-BUND:CB-K15/1437, CERT-BUND:CB-K15/0966, CERT-BUND:CB-K15/0901, CERT-BUND:CB-K15/0854, CERT-BUND:CB-K15/0806, CERT-BUND:CB-K15/0769, CERT-BUND:CB-K15/0757, CERT-BUND:CB-K15/0665, CERT-BUND:CB-K15/0482, CERT-BUND:CB-K15/0362, CERT-BUND:CB-K15/0358, CERT-BUND:CB-K15/0278, CERT-BUND:CB-K15/0222, DFN-CERT:DFN-CERT-2016-1004, DFN-CERT:DFN-CERT-2015-1644, DFN-CERT:DFN-CERT-2015-1514, DFN-CERT:DFN-CERT-2015-1017, DFN-CERT:DFN-CERT-2015-0956, DFN-CERT:DFN-CERT-2015-0900, DFN-CERT:DFN-CERT-2015-0842, DFN-CERT:DFN-CERT-2015-0809, DFN-CERT:DFN-CERT-2015-0794, DFN-CERT:DFN-CERT-2015-0697, DFN-CERT:DFN-CERT-2015-0505, DFN-CERT:DFN-CERT-2015-0371, DFN-CERT:DFN-CERT-2015-0370, DFN-CERT:DFN-CERT-2015-0286, DFN-CERT:DFN-CERT-2015-0228 |

## Scanner evidence for A206

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K15/1437, CERT-BUND:CB-K15/0757, CERT-BUND:CB-K15/0552, CERT-BUND:CB-K15/0459, CERT-BUND:CB-K15/0207, DFN-CERT:DFN-CERT-2019-1354, DFN-CERT:DFN-CERT-2015-1514, DFN-CERT:DFN-CERT-2015-0794, DFN-CERT:DFN-CERT-2015-0579, DFN-CERT:DFN-CERT-2015-0487, DFN-CERT:DFN-CERT-2015-0212 |

## Scanner evidence for A207

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2025-0479, CERT-BUND:CB-K15/1360, CERT-BUND:CB-K15/0714, DFN-CERT:DFN-CERT-2015-1435, DFN-CERT:DFN-CERT-2015-0749 |

## Scanner evidence for A208

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K16/0944, CERT-BUND:CB-K16/0912, CERT-BUND:CB-K16/0623, CERT-BUND:CB-K16/0422, CERT-BUND:CB-K16/0161, CERT-BUND:CB-K16/0136, CERT-BUND:CB-K15/1792, CERT-BUND:CB-K15/1453, DFN-CERT:DFN-CERT-2016-1004, DFN-CERT:DFN-CERT-2016-0972, DFN-CERT:DFN-CERT-2016-0676, DFN-CERT:DFN-CERT-2016-0460, DFN-CERT:DFN-CERT-2016-0176, DFN-CERT:DFN-CERT-2016-0154, DFN-CERT:DFN-CERT-2015-1898, DFN-CERT:DFN-CERT-2015-1530 |

## Scanner evidence for A209

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K16/0944, CERT-BUND:CB-K16/0422, CERT-BUND:CB-K15/1571, CERT-BUND:CB-K15/1439, CERT-BUND:CB-K15/1415, CERT-BUND:CB-K15/1261, DFN-CERT:DFN-CERT-2016-1004, DFN-CERT:DFN-CERT-2016-0460, DFN-CERT:DFN-CERT-2015-1658, DFN-CERT:DFN-CERT-2015-1515, DFN-CERT:DFN-CERT-2015-1493, DFN-CERT:DFN-CERT-2015-1335 |

## Scanner evidence for A210

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | |

CERT-BUND:CB-K16/1776, CERT-BUND:CB-K16/0614, CERT-BUND:CB-K16/0161, CERT-BUND:CB-K16/0136, DFN-CERT:DFN-CERT-2016-1882, DFN-CERT:DFN-CERT-2016-0659, DFN-CERT:DFN-CERT-2016-0176, DFN-CERT:DFN-CERT-2016-0154

## Scanner evidence for A211

The action above covers the following detailed scanner evidence.

Vendor references

CERT-BUND:WID-SEC-2025-1425, CERT-BUND:CB-K16/0944, CERT-BUND:CB-K16/0422, CERT-BUND:CB-K15/1571, CERT-BUND:CB-K15/1561, CERT-BUND:CB-K15/1478, CERT-BUND:CB-K15/1439, CERT-BUND:CB-K15/1415, CERT-BUND:CB-K15/1337, DFN-CERT:DFN-CERT-2016-1004, DFN-CERT:DFN-CERT-2016-0460, DFN-CERT:DFN-CERT-2015-1658, DFN-CERT:DFN-CERT-2015-1644, DFN-CERT:DFN-CERT-2015-1556, DFN-CERT:DFN-CERT-2015-1515, DFN-CERT:DFN-CERT-2015-1493, DFN-CERT:DFN-CERT-2015-1407

## Scanner evidence for A212

The action above covers the following detailed scanner evidence.

Vendor references

CERT-BUND:CB-K16/0944, CERT-BUND:CB-K16/0912, CERT-BUND:CB-K16/0623, CERT-BUND:CB-K16/0614, CERT-BUND:CB-K16/0422, CERT-BUND:CB-K15/1439, CERT-BUND:CB-K15/1261, CERT-BUND:CB-K15/1147, DFN-CERT:DFN-CERT-2016-1004, DFN-CERT:DFN-CERT-2016-0972, DFN-CERT:DFN-CERT-2016-0676, DFN-CERT:DFN-CERT-2016-0659, DFN-CERT:DFN-CERT-2016-0460, DFN-CERT:DFN-CERT-2015-1515, DFN-CERT:DFN-CERT-2015-1335, DFN-CERT:DFN-CERT-2015-1203

## Scanner evidence for A213

The action above covers the following detailed scanner evidence.

Vendor references

CERT-BUND:CB-K16/1366, CERT-BUND:CB-K16/0361, CERT-BUND:CB-K16/0237, DFN-CERT:DFN-CERT-2019-1285, DFN-CERT:DFN-CERT-2016-1457, DFN-CERT:DFN-CERT-2016-0401, DFN-CERT:DFN-CERT-2016-0257

## Scanner evidence for A214

The action above covers the following detailed scanner evidence.

Vendor references

CERT-BUND:CB-K19/1015, CERT-BUND:CB-K16/0870, CERT-BUND:CB-K16/0596, CERT-BUND:CB-K16/0589, CERT-BUND:CB-K16/0572, CERT-BUND:CB-K16/0550, CERT-BUND:CB-K16/0546, DFN-CERT:DFN-CERT-2019-2479, DFN-CERT:DFN-CERT-2016-0930, DFN-CERT:DFN-CERT-2016-0905, DFN-CERT:DFN-CERT-2016-0648, DFN-CERT:DFN-CERT-2016-0639, DFN-CERT:DFN-CERT-2016-0620, DFN-CERT:DFN-CERT-2016-0591, DFN-CERT:DFN-CERT-2016-0589

## Scanner evidence for A215

The action above covers the following detailed scanner evidence.

Vendor references

CERT-BUND:CB-K16/1776, CERT-BUND:CB-K16/1620, CERT-BUND:CB-K16/0944, CERT-BUND:CB-K16/0912, CERT-BUND:CB-K16/0723, CERT-BUND:CB-K16/0623, CERT-BUND:CB-K16/0614, DFN-CERT:DFN-CERT-2016-1882, DFN-CERT:DFN-CERT-2016-1717, DFN-CERT:DFN-CERT-2016-1004, DFN-CERT:DFN-CERT-2016-0972, DFN-CERT:DFN-CERT-2016-0775, DFN-CERT:DFN-CERT-2016-0676, DFN-CERT:DFN-CERT-2016-0659

## Scanner evidence for A216

The action above covers the following detailed scanner evidence.

Vendor references

CERT-BUND:CB-K16/1776, CERT-BUND:CB-K16/1319, CERT-BUND:CB-K16/0944, CERT-BUND:CB-K16/0912, CERT-BUND:CB-K16/0884, CERT-BUND:CB-K16/0872, CERT-BUND:CB-K16/0779, CERT-BUND:CB-K16/0723, CERT-BUND:CB-K16/0705, CERT-BUND:CB-K16/0614, CERT-BUND:CB-K16/0494, DFN-CERT:DFN-CERT-2018-1161, DFN-CERT:DFN-CERT-2016-1882, DFN-CERT:DFN-CERT-2016-1402, DFN-CERT:DFN-CERT-2016-1004, DFN-CERT:DFN-CERT-2016-0972, DFN-CERT:DFN-CERT-2016-0940, DFN-CERT:DFN-CERT-2016-0929, DFN-CERT:DFN-CERT-2016-0835, DFN-CERT:DFN-CERT-2016-0775, DFN-CERT:DFN-CERT-2016-0764, DFN-CERT:DFN-CERT-2016-0659, DFN-CERT:DFN-CERT-2016-0536

## Scanner evidence for A217

The action above covers the following detailed scanner evidence.

Vendor references

CERT-BUND:CB-K16/1776, CERT-BUND:CB-K16/0944, CERT-BUND:CB-K16/0912, CERT-BUND:CB-K16/0909, CERT-BUND:CB-K16/0868, CERT-BUND:CB-K16/0779, CERT-BUND:CB-K16/0774, CERT-BUND:CB-K16/0760, DFN-CERT:DFN-CERT-2016-1882, DFN-CERT:DFN-CERT-2016-1004, DFN-CERT:DFN-CERT-2016-0972, DFN-CERT:DFN-CERT-2016-0960, DFN-CERT:DFN-CERT-2016-0924, DFN-CERT:DFN-CERT-2016-0835, DFN-CERT:DFN-CERT-2016-0827, DFN-CERT:DFN-CERT-2016-0814

## Scanner evidence for A218

The action above covers the following detailed scanner evidence.

Vendor references

CERT-BUND:CB-K17/0318, CERT-BUND:CB-K16/1776, CERT-BUND:CB-K16/1190, CERT-BUND:CB-K16/1179, CERT-BUND:CB-K16/0944, CERT-BUND:CB-K16/0937, CERT-BUND:CB-K16/0912, CERT-BUND:CB-K16/0911, CERT-BUND:CB-K16/0868, CERT-BUND:CB-K16/0705, CERT-BUND:CB-K16/0623, CERT-BUND:CB-K16/0614, DFN-CERT:DFN-CERT-2017-0325, DFN-CERT:DFN-CERT-2016-1882, DFN-CERT:DFN-CERT-2016-1265, DFN-CERT:DFN-CERT-2016-1253, DFN-CERT:DFN-CERT-2016-1004, DFN-CERT:DFN-CERT-2016-0996, DFN-CERT:DFN-CERT-2016-0972, DFN-CERT:DFN-CERT-2016-0944, DFN-CERT:DFN-CERT-2016-0924, DFN-CERT:DFN-CERT-2016-0764, DFN-CERT:DFN-CERT-2016-0676, DFN-CERT:DFN-CERT-2016-0659

## Scanner evidence for A219

The action above covers the following detailed scanner evidence.

Vendor references

CERT-BUND:CB-K16/1776, CERT-BUND:CB-K16/0944, CERT-BUND:CB-K16/0912, CERT-BUND:CB-K16/0868, CERT-BUND:CB-K16/0779, CERT-BUND:CB-K16/0760, CERT-BUND:CB-K16/0623, CERT-BUND:CB-K16/0614, CERT-BUND:CB-K16/0405, DFN-CERT:DFN-CERT-2016-1882, DFN-CERT:DFN-CERT-2016-1004, DFN-CERT:DFN-CERT-2016-0972, DFN-CERT:DFN-CERT-2016-0924, DFN-CERT:DFN-CERT-2016-0835, DFN-CERT:DFN-CERT-2016-0814, DFN-CERT:DFN-CERT-2016-0676, DFN-CERT:DFN-CERT-2016-0659, DFN-CERT:DFN-CERT-2016-0441

## Scanner evidence for A220

The action above covers the following detailed scanner evidence.

Vendor references

CERT-BUND:CB-K16/1776, CERT-BUND:CB-K16/0796, CERT-BUND:CB-K16/0779, CERT-BUND:CB-K16/0760, DFN-CERT:DFN-CERT-2016-1882, DFN-CERT:DFN-CERT-2016-0847, DFN-CERT:DFN-CERT-2016-0835, DFN-CERT:DFN-CERT-2016-0814

## Scanner evidence for A222

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K18/0028, CERT-BUND:CB-K16/1776, CERT-BUND:CB-K16/0944, CERT-BUND:CB-K16/0912, CERT-BUND:CB-K16/0705, CERT-BUND:CB-K16/0614, DFN-CERT:DFN-CERT-2018-0010, DFN-CERT:DFN-CERT-2016-1882, DFN-CERT:DFN-CERT-2016-1004, DFN-CERT:DFN-CERT-2016-0972, DFN-CERT:DFN-CERT-2016-0764, DFN-CERT:DFN-CERT-2016-0659 |

## Scanner evidence for A223

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2025-1425, CERT-BUND:CB-K16/1776, CERT-BUND:CB-K16/0944, CERT-BUND:CB-K16/0912, CERT-BUND:CB-K16/0623, CERT-BUND:CB-K16/0614, CERT-BUND:CB-K16/0422, CERT-BUND:CB-K15/1571, CERT-BUND:CB-K15/1561, CERT-BUND:CB-K15/1478, CERT-BUND:CB-K15/1439, CERT-BUND:CB-K15/1415, CERT-BUND:CB-K15/1337, DFN-CERT:DFN-CERT-2016-1882, DFN-CERT:DFN-CERT-2016-1004, DFN-CERT:DFN-CERT-2016-0972, DFN-CERT:DFN-CERT-2016-0676, DFN-CERT:DFN-CERT-2016-0659, DFN-CERT:DFN-CERT-2016-0460, DFN-CERT:DFN-CERT-2015-1658, DFN-CERT:DFN-CERT-2015-1644, DFN-CERT:DFN-CERT-2015-1556, DFN-CERT:DFN-CERT-2015-1515, DFN-CERT:DFN-CERT-2015-1493, DFN-CERT:DFN-CERT-2015-1407 |

## Scanner evidence for A224

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2025-2522, CERT-BUND:CB-K17/1252, CERT-BUND:CB-K16/1941, CERT-BUND:CB-K16/1854, CERT-BUND:CB-K16/1776, CERT-BUND:CB-K16/1549, CERT-BUND:CB-K16/1499, CERT-BUND:CB-K16/1407, CERT-BUND:CB-K16/1283, CERT-BUND:CB-K16/1248, CERT-BUND:CB-K16/1179, CERT-BUND:CB-K16/1115, CERT-BUND:CB-K16/1110, CERT-BUND:CB-K16/1106, CERT-BUND:CB-K16/1092, CERT-BUND:CB-K16/1077, CERT-BUND:CB-K16/1045, DFN-CERT:DFN-CERT-2017-1295, DFN-CERT:DFN-CERT-2016-2047, DFN-CERT:DFN-CERT-2016-1961, DFN-CERT:DFN-CERT-2016-1882, DFN-CERT:DFN-CERT-2016-1641, DFN-CERT:DFN-CERT-2016-1590, DFN-CERT:DFN-CERT-2016-1498, DFN-CERT:DFN-CERT-2016-1367, DFN-CERT:DFN-CERT-2016-1326, DFN-CERT:DFN-CERT-2016-1253, DFN-CERT:DFN-CERT-2016-1184, DFN-CERT:DFN-CERT-2016-1179, DFN-CERT:DFN-CERT-2016-1178, DFN-CERT:DFN-CERT-2016-1157, DFN-CERT:DFN-CERT-2016-1144, DFN-CERT:DFN-CERT-2016-1110 |

## Scanner evidence for A225

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2025-2522, CERT-BUND:WID-SEC-2025-0370, CERT-BUND:CB-K17/2013, CERT-BUND:CB-K17/1854, CERT-BUND:CB-K17/1842, CERT-BUND:CB-K17/1622, CERT-BUND:CB-K17/0527, CERT-BUND:CB-K17/0055, CERT-BUND:CB-K16/1995, CERT-BUND:CB-K16/1620, CERT-BUND:CB-K16/1289, CERT-BUND:CB-K16/1103, CERT-BUND:CB-K16/1088, CERT-BUND:CB-K16/1087, DFN-CERT:DFN-CERT-2017-2104, DFN-CERT:DFN-CERT-2017-1926, DFN-CERT:DFN-CERT-2017-1925, DFN-CERT:DFN-CERT-2017-1692, DFN-CERT:DFN-CERT-2017-0532, DFN-CERT:DFN-CERT-2017-0060, DFN-CERT:DFN-CERT-2016-2108, DFN-CERT:DFN-CERT-2016-1717, DFN-CERT:DFN-CERT-2016-1372, DFN-CERT:DFN-CERT-2016-1175, DFN-CERT:DFN-CERT-2016-1162, DFN-CERT:DFN-CERT-2016-1153 |

## Scanner evidence for A226

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K17/1252, CERT-BUND:CB-K17/1011, CERT-BUND:CB-K16/1776, CERT-BUND:CB-K16/1722, CERT-BUND:CB-K16/1549, CERT-BUND:CB-K16/1499, CERT-BUND:CB-K16/1458, CERT-BUND:CB-K16/1452, CERT-BUND:CB-K16/1440, CERT-BUND:CB-K16/1407, CERT-BUND:CB-K16/1345, CERT-BUND:CB-K16/1283, CERT-BUND:CB-K16/1257, CERT- |

BUND:CB-K16/1248, CERT-BUND:CB-K16/1235, CERT-BUND:CB-K16/1233, CERT-BUND:CB-K16/1179, CERT-BUND:CB-K16/1130, CERT-BUND:CB-K16/1115, CERT-BUND:CB-K16/1110, DFN-CERT:DFN-CERT-2017-1295, DFN-CERT:DFN-CERT-2017-1046, DFN-CERT:DFN-CERT-2016-1882, DFN-CERT:DFN-CERT-2016-1822, DFN-CERT:DFN-CERT-2016-1641, DFN-CERT:DFN-CERT-2016-1590, DFN-CERT:DFN-CERT-2016-1541, DFN-CERT:DFN-CERT-2016-1536, DFN-CERT:DFN-CERT-2016-1526, DFN-CERT:DFN-CERT-2016-1498, DFN-CERT:DFN-CERT-2016-1431, DFN-CERT:DFN-CERT-2016-1367, DFN-CERT:DFN-CERT-2016-1335, DFN-CERT:DFN-CERT-2016-1326, DFN-CERT:DFN-CERT-2016-1310, DFN-CERT:DFN-CERT-2016-1309, DFN-CERT:DFN-CERT-2016-1253, DFN-CERT:DFN-CERT-2016-1203, DFN-CERT:DFN-CERT-2016-1184, DFN-CERT:DFN-CERT-2016-1179

## Scanner evidence for A227

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K16/1242, DFN-CERT:DFN-CERT-2017-1382, DFN-CERT:DFN-CERT-2016-1317 |

## Scanner evidence for A228

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K16/0944, CERT-BUND:CB-K16/0912, CERT-BUND:CB-K16/0623, CERT-BUND:CB-K16/0614, DFN-CERT:DFN-CERT-2016-1004, DFN-CERT:DFN-CERT-2016-0972, DFN-CERT:DFN-CERT-2016-0676, DFN-CERT:DFN-CERT-2016-0659 |

## Scanner evidence for A229

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K16/1179, CERT-BUND:CB-K16/0944, CERT-BUND:CB-K16/0912, CERT-BUND:CB-K16/0911, CERT-BUND:CB-K16/0868, DFN-CERT:DFN-CERT-2016-1253, DFN-CERT:DFN-CERT-2016-1004, DFN-CERT:DFN-CERT-2016-0972, DFN-CERT:DFN-CERT-2016-0944, DFN-CERT:DFN-CERT-2016-0924 |

## Scanner evidence for A230

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K16/0944, CERT-BUND:CB-K15/1261, CERT-BUND:CB-K15/1158, CERT-BUND:CB-K15/1031, CERT-BUND:CB-K15/0973, CERT-BUND:CB-K15/0966, CERT-BUND:CB-K15/0942, CERT-BUND:CB-K15/0936, CERT-BUND:CB-K15/0880, CERT-BUND:CB-K15/0854, DFN-CERT:DFN-CERT-2016-1004, DFN-CERT:DFN-CERT-2015-1335, DFN-CERT:DFN-CERT-2015-1217, DFN-CERT:DFN-CERT-2015-1083, DFN-CERT:DFN-CERT-2015-1021, DFN-CERT:DFN-CERT-2015-1017, DFN-CERT:DFN-CERT-2015-0989, DFN-CERT:DFN-CERT-2015-0983, DFN-CERT:DFN-CERT-2015-0926, DFN-CERT:DFN-CERT-2015-0900 |

## Scanner evidence for A231

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K17/1575, CERT-BUND:CB-K17/1461, CERT-BUND:CB-K17/1252, CERT-BUND:CB-K16/1868, CERT-BUND:CB-K16/1776, CERT-BUND:CB-K16/1722, CERT-BUND:CB-K16/1629, CERT-BUND:CB-K16/1600, CERT-BUND:CB-K16/1452, CERT-BUND:CB-K16/1257, CERT-BUND:CB-K16/1230, CERT-BUND:CB-K16/1179, CERT-BUND:CB-K16/1115, CERT-BUND:CB-K16/1106, CERT-BUND:CB-K16/1077, CERT-BUND:CB-K16/1070, CERT-BUND:CB-K16/1045, CERT-BUND:CB-K16/1030, CERT-BUND:CB-K16/0975, CERT-BUND:CB-K16/0966, CERT-BUND:CB-K16/0965, DFN-CERT:DFN-CERT-2021-0715, DFN-CERT:DFN-CERT-2020-2741, DFN-CERT:DFN-CERT-2018-0576, DFN-CERT:DFN-CERT-2017-1647, DFN-CERT:DFN- |

CERT-2017-1529, DFN-CERT:DFN-CERT-2017-1295, DFN-CERT:DFN-CERT-2016-1974, DFN-CERT:DFN-CERT-2016-1882, DFN-CERT:DFN-CERT-2016-1822, DFN-CERT:DFN-CERT-2016-1729, DFN-CERT:DFN-CERT-2016-1697, DFN-CERT:DFN-CERT-2016-1541, DFN-CERT:DFN-CERT-2016-1335, DFN-CERT:DFN-CERT-2016-1295, DFN-CERT:DFN-CERT-2016-1253, DFN-CERT:DFN-CERT-2016-1184, DFN-CERT:DFN-CERT-2016-1178, DFN-CERT:DFN-CERT-2016-1144, DFN-CERT:DFN-CERT-2016-1139, DFN-CERT:DFN-CERT-2016-1110, DFN-CERT:DFN-CERT-2016-1097, DFN-CERT:DFN-CERT-2016-1033, DFN-CERT:DFN-CERT-2016-1022, DFN-CERT:DFN-CERT-2016-1021

## Scanner evidence for A232

The action above covers the following detailed scanner evidence.

Vendor references

CERT-BUND:CB-K16/2012, CERT-BUND:CB-K16/1776, CERT-BUND:CB-K16/1452, CERT-BUND:CB-K16/1179, CERT-BUND:CB-K16/1106, CERT-BUND:CB-K16/1070, CERT-BUND:CB-K16/1030, CERT-BUND:CB-K16/0965, DFN-CERT:DFN-CERT-2018-0576, DFN-CERT:DFN-CERT-2016-2125, DFN-CERT:DFN-CERT-2016-1882, DFN-CERT:DFN-CERT-2016-1541, DFN-CERT:DFN-CERT-2016-1253, DFN-CERT:DFN-CERT-2016-1178, DFN-CERT:DFN-CERT-2016-1139, DFN-CERT:DFN-CERT-2016-1097, DFN-CERT:DFN-CERT-2016-1022

## Scanner evidence for A233

The action above covers the following detailed scanner evidence.

Vendor references

CERT-BUND:CB-K16/1982, CERT-BUND:CB-K16/1776, CERT-BUND:CB-K16/1179, CERT-BUND:CB-K16/0944, CERT-BUND:CB-K16/0937, CERT-BUND:CB-K16/0912, CERT-BUND:CB-K16/0911, CERT-BUND:CB-K16/0909, CERT-BUND:CB-K16/0796, DFN-CERT:DFN-CERT-2016-2084, DFN-CERT:DFN-CERT-2016-1882, DFN-CERT:DFN-CERT-2016-1253, DFN-CERT:DFN-CERT-2016-1004, DFN-CERT:DFN-CERT-2016-0996, DFN-CERT:DFN-CERT-2016-0972, DFN-CERT:DFN-CERT-2016-0960, DFN-CERT:DFN-CERT-2016-0944, DFN-CERT:DFN-CERT-2016-0847

## Scanner evidence for A234

The action above covers the following detailed scanner evidence.

Vendor references

CERT-BUND:CB-K16/1776, CERT-BUND:CB-K16/1179, CERT-BUND:CB-K16/1045, CERT-BUND:CB-K16/0944, CERT-BUND:CB-K16/0937, CERT-BUND:CB-K16/0912, CERT-BUND:CB-K16/0911, CERT-BUND:CB-K16/0909, CERT-BUND:CB-K16/0801, CERT-BUND:CB-K16/0796, DFN-CERT:DFN-CERT-2016-1882, DFN-CERT:DFN-CERT-2016-1253, DFN-CERT:DFN-CERT-2016-1110, DFN-CERT:DFN-CERT-2016-1004, DFN-CERT:DFN-CERT-2016-0996, DFN-CERT:DFN-CERT-2016-0972, DFN-CERT:DFN-CERT-2016-0960, DFN-CERT:DFN-CERT-2016-0944, DFN-CERT:DFN-CERT-2016-0857, DFN-CERT:DFN-CERT-2016-0847

## Scanner evidence for A235

The action above covers the following detailed scanner evidence.

Vendor references

CERT-BUND:CB-K16/1614, CERT-BUND:CB-K16/1257, CERT-BUND:CB-K16/1230, CERT-BUND:CB-K16/1179, CERT-BUND:CB-K16/1106, CERT-BUND:CB-K16/1030, DFN-CERT:DFN-CERT-2016-1719, DFN-CERT:DFN-CERT-2016-1335, DFN-CERT:DFN-CERT-2016-1295, DFN-CERT:DFN-CERT-2016-1253, DFN-CERT:DFN-CERT-2016-1178, DFN-CERT:DFN-CERT-2016-1097

## Scanner evidence for A236

The action above covers the following detailed scanner evidence.

Vendor references

CERT-BUND:CB-K16/1776, CERT-BUND:CB-K16/1179, CERT-BUND:CB-K16/0944, CERT-BUND:CB-K16/0912, CERT-BUND:CB-K16/0911, DFN-CERT:DFN-CERT-2016-1882, DFN-

CERT:DFN-CERT-2016-1253, DFN-CERT:DFN-CERT-2016-1004, DFN-CERT:DFN-CERT-2016-0972, DFN-CERT:DFN-CERT-2016-0944

## Scanner evidence for A237

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2023-0450, CERT-BUND:WID-SEC-2023-0449, CERT-BUND:CB-K18/0041, CERT-BUND:CB-K17/2219, CERT-BUND:CB-K17/2112, CERT-BUND:CB-K17/1753, CERT-BUND:CB-K17/1349, CERT-BUND:CB-K17/1292, CERT-BUND:CB-K17/0055, CERT-BUND:CB-K16/1837, CERT-BUND:CB-K16/1629, CERT-BUND:CB-K16/1487, CERT-BUND:CB-K16/1485, CERT-BUND:CB-K16/1252, CERT-BUND:CB-K16/1221, CERT-BUND:CB-K16/1082, DFN-CERT:DFN-CERT-2023-1920, DFN-CERT:DFN-CERT-2019-1408, DFN-CERT:DFN-CERT-2018-1828, DFN-CERT:DFN-CERT-2018-1070, DFN-CERT:DFN-CERT-2018-0046, DFN-CERT:DFN-CERT-2017-2320, DFN-CERT:DFN-CERT-2017-2208, DFN-CERT:DFN-CERT-2017-1831, DFN-CERT:DFN-CERT-2017-1407, DFN-CERT:DFN-CERT-2017-1340, DFN-CERT:DFN-CERT-2017-0060, DFN-CERT:DFN-CERT-2016-1943, DFN-CERT:DFN-CERT-2016-1729, DFN-CERT:DFN-CERT-2016-1576, DFN-CERT:DFN-CERT-2016-1574, DFN-CERT:DFN-CERT-2016-1331, DFN-CERT:DFN-CERT-2016-1243, DFN-CERT:DFN-CERT-2016-1149 |

## Scanner evidence for A238

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K16/1958, CERT-BUND:CB-K16/1549, CERT-BUND:CB-K16/1543, CERT-BUND:CB-K16/1532, CERT-BUND:CB-K16/1426, DFN-CERT:DFN-CERT-2018-0835, DFN-CERT:DFN-CERT-2016-2063, DFN-CERT:DFN-CERT-2016-1641, DFN-CERT:DFN-CERT-2016-1639, DFN-CERT:DFN-CERT-2016-1631, DFN-CERT:DFN-CERT-2016-1495 |

## Scanner evidence for A239

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K16/1776, CERT-BUND:CB-K16/1772, CERT-BUND:CB-K16/1549, CERT-BUND:CB-K16/1543, CERT-BUND:CB-K16/1532, CERT-BUND:CB-K16/1499, CERT-BUND:CB-K16/1440, CERT-BUND:CB-K16/1280, DFN-CERT:DFN-CERT-2016-1882, DFN-CERT:DFN-CERT-2016-1878, DFN-CERT:DFN-CERT-2016-1641, DFN-CERT:DFN-CERT-2016-1639, DFN-CERT:DFN-CERT-2016-1631, DFN-CERT:DFN-CERT-2016-1590, DFN-CERT:DFN-CERT-2016-1526, DFN-CERT:DFN-CERT-2016-1359 |

## Scanner evidence for A240

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K17/0327, CERT-BUND:CB-K17/0269, CERT-BUND:CB-K16/1941, CERT-BUND:CB-K16/1868, CERT-BUND:CB-K16/1854, CERT-BUND:CB-K16/1811, CERT-BUND:CB-K16/1645, CERT-BUND:CB-K16/1606, CERT-BUND:CB-K16/1603, DFN-CERT:DFN-CERT-2017-0334, DFN-CERT:DFN-CERT-2017-0274, DFN-CERT:DFN-CERT-2016-2047, DFN-CERT:DFN-CERT-2016-1974, DFN-CERT:DFN-CERT-2016-1961, DFN-CERT:DFN-CERT-2016-1918, DFN-CERT:DFN-CERT-2016-1745, DFN-CERT:DFN-CERT-2016-1704, DFN-CERT:DFN-CERT-2016-1700 |

## Scanner evidence for A241

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2023-1996, CERT-BUND:CB-K18/0919, CERT-BUND:CB-K18/0591, CERT-BUND:CB-K18/0137, CERT-BUND:CB-K18/0041, CERT-BUND:CB-K17/2219, CERT-BUND:CB-K17/2112, CERT-BUND:CB-K17/1292, CERT-BUND:CB-K17/1061, CERT-BUND:CB-K17/0527, |

CERT-BUND:CB-K17/0377, CERT-BUND:CB-K17/0127, CERT-BUND:CB-K17/0041, CERT-BUND:CB-K16/1991, DFN-CERT:DFN-CERT-2021-0776, DFN-CERT:DFN-CERT-2019-1408, DFN-CERT:DFN-CERT-2018-2259, DFN-CERT:DFN-CERT-2018-2191, DFN-CERT:DFN-CERT-2018-2068, DFN-CERT:DFN-CERT-2018-1828, DFN-CERT:DFN-CERT-2018-1568, DFN-CERT:DFN-CERT-2018-1432, DFN-CERT:DFN-CERT-2018-1112, DFN-CERT:DFN-CERT-2018-1070, DFN-CERT:DFN-CERT-2018-1068, DFN-CERT:DFN-CERT-2018-0150, DFN-CERT:DFN-CERT-2018-0046, DFN-CERT:DFN-CERT-2017-2320, DFN-CERT:DFN-CERT-2017-2208, DFN-CERT:DFN-CERT-2017-1340, DFN-CERT:DFN-CERT-2017-1096, DFN-CERT:DFN-CERT-2017-0532, DFN-CERT:DFN-CERT-2017-0386, DFN-CERT:DFN-CERT-2017-0130, DFN-CERT:DFN-CERT-2017-0042, DFN-CERT:DFN-CERT-2016-2099

## Scanner evidence for A242

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K20/0857, CERT-BUND:CB-K17/0602, DFN-CERT:DFN-CERT-2020-0072, DFN-CERT:DFN-CERT-2019-1655, DFN-CERT:DFN-CERT-2018-1416, DFN-CERT:DFN-CERT-2017-0621 |

## Scanner evidence for A243

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K16/1485, CERT-BUND:CB-K16/0694, CERT-BUND:CB-K16/0684, CERT-BUND:CB-K16/0449, CERT-BUND:CB-K16/0162, DFN-CERT:DFN-CERT-2018-1828, DFN-CERT:DFN-CERT-2016-1574, DFN-CERT:DFN-CERT-2016-0754, DFN-CERT:DFN-CERT-2016-0733, DFN-CERT:DFN-CERT-2016-0488, DFN-CERT:DFN-CERT-2016-0182 |

## Scanner evidence for A244

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2023-2719, CERT-BUND:WID-SEC-2023-2718, CERT-BUND:CB-K18/0270, CERT-BUND:CB-K18/0048, CERT-BUND:CB-K17/2123, CERT-BUND:CB-K17/1575, CERT-BUND:CB-K17/1573, CERT-BUND:CB-K17/1562, CERT-BUND:CB-K17/1468, CERT-BUND:CB-K17/1461, CERT-BUND:CB-K17/1373, CERT-BUND:CB-K17/1358, CERT-BUND:CB-K17/1132, CERT-BUND:CB-K17/1011, CERT-BUND:CB-K17/0908, DFN-CERT:DFN-CERT-2020-1221, DFN-CERT:DFN-CERT-2020-0484, DFN-CERT:DFN-CERT-2020-0479, DFN-CERT:DFN-CERT-2019-1052, DFN-CERT:DFN-CERT-2018-2116, DFN-CERT:DFN-CERT-2018-0835, DFN-CERT:DFN-CERT-2018-0733, DFN-CERT:DFN-CERT-2018-0290, DFN-CERT:DFN-CERT-2018-0055, DFN-CERT:DFN-CERT-2017-2219, DFN-CERT:DFN-CERT-2017-1647, DFN-CERT:DFN-CERT-2017-1644, DFN-CERT:DFN-CERT-2017-1629, DFN-CERT:DFN-CERT-2017-1530, DFN-CERT:DFN-CERT-2017-1529, DFN-CERT:DFN-CERT-2017-1432, DFN-CERT:DFN-CERT-2017-1420, DFN-CERT:DFN-CERT-2017-1161, DFN-CERT:DFN-CERT-2017-1046, DFN-CERT:DFN-CERT-2017-0932 |

## Scanner evidence for A245

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K18/0048, CERT-BUND:CB-K17/1461, CERT-BUND:CB-K17/1132, DFN-CERT:DFN-CERT-2018-0055, DFN-CERT:DFN-CERT-2017-1529, DFN-CERT:DFN-CERT-2017-1161 |

## Scanner evidence for A246

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K17/1575, CERT-BUND:CB-K17/1461, CERT-BUND:CB-K17/1358, CERT-BUND:CB-K17/1252, CERT-BUND:CB-K17/0269, CERT-BUND:CB-K17/0124, CERT-BUND:CB-K17/0053, CERT-BUND:CB-K17/0015, CERT-BUND:CB-K16/2015, CERT-BUND:CB-K16/2011, |

CERT-BUND:CB-K16/1943, CERT-BUND:CB-K16/1790, CERT-BUND:CB-K16/1606, DFN-CERT:DFN-CERT-2019-2707, DFN-CERT:DFN-CERT-2018-0835, DFN-CERT:DFN-CERT-2017-1647, DFN-CERT:DFN-CERT-2017-1529, DFN-CERT:DFN-CERT-2017-1420, DFN-CERT:DFN-CERT-2017-1295, DFN-CERT:DFN-CERT-2017-0274, DFN-CERT:DFN-CERT-2017-0131, DFN-CERT:DFN-CERT-2017-0058, DFN-CERT:DFN-CERT-2017-0016, DFN-CERT:DFN-CERT-2016-2130, DFN-CERT:DFN-CERT-2016-2123, DFN-CERT:DFN-CERT-2016-2053, DFN-CERT:DFN-CERT-2016-1887, DFN-CERT:DFN-CERT-2016-1704

## Scanner evidence for A247

The action above covers the following detailed scanner evidence.

Vendor references: CERT-BUND:CB-K18/0478, CERT-BUND:CB-K17/2077, CERT-BUND:CB-K17/1876, CERT-BUND:CB-K17/1603, DFN-CERT:DFN-CERT-2018-0513, DFN-CERT:DFN-CERT-2017-2172, DFN-CERT:DFN-CERT-2017-1953, DFN-CERT:DFN-CERT-2017-1671

## Scanner evidence for A248

The action above covers the following detailed scanner evidence.

Vendor references: CERT-BUND:WID-SEC-2024-1082, CERT-BUND:CB-K20/0041, CERT-BUND:CB-K18/0137, CERT-BUND:CB-K17/2126, CERT-BUND:CB-K17/2014, CERT-BUND:CB-K17/2002, DFN-CERT:DFN-CERT-2024-1260, DFN-CERT:DFN-CERT-2019-0362, DFN-CERT:DFN-CERT-2018-2554, DFN-CERT:DFN-CERT-2018-2191, DFN-CERT:DFN-CERT-2018-2068, DFN-CERT:DFN-CERT-2018-1828, DFN-CERT:DFN-CERT-2018-1568, DFN-CERT:DFN-CERT-2018-0150, DFN-CERT:DFN-CERT-2017-2217, DFN-CERT:DFN-CERT-2017-2100, DFN-CERT:DFN-CERT-2017-2093

## Scanner evidence for A249

The action above covers the following detailed scanner evidence.

Vendor references: CERT-BUND:CB-K18/0270, CERT-BUND:CB-K18/0048, CERT-BUND:CB-K17/2123, DFN-CERT:DFN-CERT-2019-1737, DFN-CERT:DFN-CERT-2018-0835, DFN-CERT:DFN-CERT-2018-0733, DFN-CERT:DFN-CERT-2018-0290, DFN-CERT:DFN-CERT-2018-0055, DFN-CERT:DFN-CERT-2017-2219

## Scanner evidence for A250

The action above covers the following detailed scanner evidence.

Vendor references: CERT-BUND:CB-K18/0498, CERT-BUND:CB-K18/0350, DFN-CERT:DFN-CERT-2019-1052, DFN-CERT:DFN-CERT-2018-0576, DFN-CERT:DFN-CERT-2018-0537, DFN-CERT:DFN-CERT-2018-0380

## Scanner evidence for A251

The action above covers the following detailed scanner evidence.

Vendor references: DFN-CERT:DFN-CERT-2022-2638, DFN-CERT:DFN-CERT-2022-0485, DFN-CERT:DFN-CERT-2022-0455, DFN-CERT:DFN-CERT-2022-0431, DFN-CERT:DFN-CERT-2020-0337, DFN-CERT:DFN-CERT-2018-1882

## Scanner evidence for A252

The action above covers the following detailed scanner evidence.

Vendor references: CERT-BUND:WID-SEC-2024-0991, CERT-BUND:WID-SEC-2024-0990, CERT-BUND:CB-K20/0307, CERT-BUND:CB-K18/0498, CERT-BUND:CB-K18/0270, CERT-BUND:CB-K18/0188, CERT-BUND:CB-K18/0174, DFN-CERT:DFN-CERT-2020-0774, DFN-CERT:DFN-CERT-2020-0680, DFN-CERT:DFN-CERT-2019-1737, DFN-CERT:DFN-CERT-2019-0362, DFN-CERT:DFN-

CERT-2019-0212, DFN-CERT:DFN-CERT-2019-0204, DFN-CERT:DFN-CERT-2018-1739, DFN-CERT:DFN-CERT-2018-0835, DFN-CERT:DFN-CERT-2018-0733, DFN-CERT:DFN-CERT-2018-0576, DFN-CERT:DFN-CERT-2018-0537, DFN-CERT:DFN-CERT-2018-0290, DFN-CERT:DFN-CERT-2018-0205, DFN-CERT:DFN-CERT-2018-0191

## Scanner evidence for A253

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K18/0698, CERT-BUND:CB-K18/0498, CERT-BUND:CB-K18/0383, DFN-CERT:DFN-CERT-2020-0680, DFN-CERT:DFN-CERT-2019-1737, DFN-CERT:DFN-CERT-2018-1232, DFN-CERT:DFN-CERT-2018-1059, DFN-CERT:DFN-CERT-2018-0733, DFN-CERT:DFN-CERT-2018-0576, DFN-CERT:DFN-CERT-2018-0537, DFN-CERT:DFN-CERT-2018-0399 |

## Scanner evidence for A254

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K18/0633, DFN-CERT:DFN-CERT-2020-0680, DFN-CERT:DFN-CERT-2019-1737, DFN-CERT:DFN-CERT-2018-1232, DFN-CERT:DFN-CERT-2018-0920, DFN-CERT:DFN-CERT-2018-0877 |

## Scanner evidence for A255

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K18/0633, DFN-CERT:DFN-CERT-2019-1737, DFN-CERT:DFN-CERT-2018-1232, DFN-CERT:DFN-CERT-2018-0920, DFN-CERT:DFN-CERT-2018-0877 |

## Scanner evidence for A256

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K18/0744, DFN-CERT:DFN-CERT-2018-1207 |

## Scanner evidence for A257

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2024-1082, CERT-BUND:CB-K20/0041, CERT-BUND:CB-K18/1031, CERT-BUND:CB-K18/0873, DFN-CERT:DFN-CERT-2024-1260, DFN-CERT:DFN-CERT-2021-2178, DFN-CERT:DFN-CERT-2020-2189, DFN-CERT:DFN-CERT-2020-0228, DFN-CERT:DFN-CERT-2019-2046, DFN-CERT:DFN-CERT-2019-0857, DFN-CERT:DFN-CERT-2019-0362, DFN-CERT:DFN-CERT-2018-2293, DFN-CERT:DFN-CERT-2018-2259, DFN-CERT:DFN-CERT-2018-2191, DFN-CERT:DFN-CERT-2018-1806, DFN-CERT:DFN-CERT-2018-1696 |

## Scanner evidence for A258

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2022-2130, CERT-BUND:CB-K18/0838, DFN-CERT:DFN-CERT-2022-2638, DFN-CERT:DFN-CERT-2019-1737, DFN-CERT:DFN-CERT-2018-2116, DFN-CERT:DFN-CERT-2018-1882, DFN-CERT:DFN-CERT-2018-1835, DFN-CERT:DFN-CERT-2018-1834, DFN-CERT:DFN-CERT-2018-1777, DFN-CERT:DFN-CERT-2018-1655 |

## Scanner evidence for A259

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2010-0712, DFN-CERT:DFN-CERT-2009-1725, DFN-CERT:DFN-CERT-2009-1497 |

## Scanner evidence for A260

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2012-1293, DFN-CERT:DFN-CERT-2009-1408 |

## Scanner evidence for A261

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2010-0482, DFN-CERT:DFN-CERT-2009-1708, DFN-CERT:DFN-CERT-2009-1621, DFN-CERT:DFN-CERT-2009-1523, DFN-CERT:DFN-CERT-2009-1363, DFN-CERT:DFN-CERT-2009-1086 |

## Scanner evidence for A262

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2012-0618, DFN-CERT:DFN-CERT-2011-0700, DFN-CERT:DFN-CERT-2010-1647, DFN-CERT:DFN-CERT-2010-0730, DFN-CERT:DFN-CERT-2010-0446, DFN-CERT:DFN-CERT-2010-0273, DFN-CERT:DFN-CERT-2009-1809, DFN-CERT:DFN-CERT-2009-1755, DFN-CERT:DFN-CERT-2009-1725, DFN-CERT:DFN-CERT-2009-1623, DFN-CERT:DFN-CERT-2009-1603, DFN-CERT:DFN-CERT-2009-1602, DFN-CERT:DFN-CERT-2009-1507, DFN-CERT:DFN-CERT-2009-1340, DFN-CERT:DFN-CERT-2009-1326 |

## Scanner evidence for A263

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2024-3056, CERT-BUND:WID-SEC-2023-1886, CERT-BUND:WID-SEC-2023-1352, CERT-BUND:WID-SEC-2022-2251, CERT-BUND:WID-SEC-2022-2000, CERT-BUND:CB-K22/0224, CERT-BUND:CB-K21/1276, DFN-CERT:DFN-CERT-2026-2722, DFN-CERT:DFN-CERT-2025-3324, DFN-CERT:DFN-CERT-2024-2847, DFN-CERT:DFN-CERT-2024-2578, DFN-CERT:DFN-CERT-2024-1671, DFN-CERT:DFN-CERT-2023-1697, DFN-CERT:DFN-CERT-2023-1332, DFN-CERT:DFN-CERT-2022-2147, DFN-CERT:DFN-CERT-2022-0437, DFN-CERT:DFN-CERT-2021-2622 |

## Scanner evidence for A264

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2024-0528, CERT-BUND:WID-SEC-2023-2480, CERT-BUND:CB-K20/0711, CERT-BUND:CB-K20/0705, CERT-BUND:CB-K20/0693, CERT-BUND:CB-K20/0555, CERT-BUND:CB-K20/0543, CERT-BUND:CB-K20/0154, DFN-CERT:DFN-CERT-2021-1736, DFN-CERT:DFN-CERT-2020-1508, DFN-CERT:DFN-CERT-2020-1413, DFN-CERT:DFN-CERT-2020-1276, DFN-CERT:DFN-CERT-2020-1134, DFN-CERT:DFN-CERT-2020-0850, DFN-CERT:DFN-CERT-2020-0835, DFN-CERT:DFN-CERT-2020-0821, DFN-CERT:DFN-CERT-2020-0569, DFN-CERT:DFN-CERT-2020-0557, DFN-CERT:DFN-CERT-2020-0501, DFN-CERT:DFN-CERT-2020-0381 |

## Scanner evidence for A268

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | |

CERT-BUND:CB-K19/0642, DFN-CERT:DFN-CERT-2020-0072, DFN-CERT:DFN-CERT-2019-1655, DFN-CERT:DFN-CERT-2019-1515

## Scanner evidence for A270

The action above covers the following detailed scanner evidence.

Vendor references

DFN-CERT:DFN-CERT-2012-1829, DFN-CERT:DFN-CERT-2012-1380, DFN-CERT:DFN-CERT-2012-1377, DFN-CERT:DFN-CERT-2012-1156, DFN-CERT:DFN-CERT-2012-1155, DFN-CERT:DFN-CERT-2012-0956, DFN-CERT:DFN-CERT-2012-0828, DFN-CERT:DFN-CERT-2012-0815, DFN-CERT:DFN-CERT-2012-0638, DFN-CERT:DFN-CERT-2012-0451, DFN-CERT:DFN-CERT-2012-0418, DFN-CERT:DFN-CERT-2012-0354, DFN-CERT:DFN-CERT-2012-0146, DFN-CERT:DFN-CERT-2012-0142, DFN-CERT:DFN-CERT-2012-0126, DFN-CERT:DFN-CERT-2012-0095, DFN-CERT:DFN-CERT-2012-0047, DFN-CERT:DFN-CERT-2011-1844, DFN-CERT:DFN-CERT-2011-1826, DFN-CERT:DFN-CERT-2011-1804, DFN-CERT:DFN-CERT-2011-1743, DFN-CERT:DFN-CERT-2011-1738, DFN-CERT:DFN-CERT-2011-1706, DFN-CERT:DFN-CERT-2011-1628, DFN-CERT:DFN-CERT-2011-1627, DFN-CERT:DFN-CERT-2011-1619

## Scanner evidence for A280

The action above covers the following detailed scanner evidence.

Vendor references

DFN-CERT:DFN-CERT-2013-1494, DFN-CERT:DFN-CERT-2012-1316, DFN-CERT:DFN-CERT-2012-1276, DFN-CERT:DFN-CERT-2012-1268, DFN-CERT:DFN-CERT-2012-1267, DFN-CERT:DFN-CERT-2012-1266, DFN-CERT:DFN-CERT-2012-1173, DFN-CERT:DFN-CERT-2012-1101, DFN-CERT:DFN-CERT-2012-0994, DFN-CERT:DFN-CERT-2012-0993, DFN-CERT:DFN-CERT-2012-0992, DFN-CERT:DFN-CERT-2012-0920, DFN-CERT:DFN-CERT-2012-0915, DFN-CERT:DFN-CERT-2012-0914, DFN-CERT:DFN-CERT-2012-0913, DFN-CERT:DFN-CERT-2012-0907, DFN-CERT:DFN-CERT-2012-0906, DFN-CERT:DFN-CERT-2012-0900, DFN-CERT:DFN-CERT-2012-0880, DFN-CERT:DFN-CERT-2012-0878

## Scanner evidence for A290

The action above covers the following detailed scanner evidence.

Vendor references

CERT-BUND:WID-SEC-2025-0370, CERT-BUND:CB-K19/0354, CERT-BUND:CB-K18/0066, CERT-BUND:CB-K17/1854, CERT-BUND:CB-K17/1622, CERT-BUND:CB-K17/1279, CERT-BUND:CB-K17/1163, CERT-BUND:CB-K17/0955, CERT-BUND:CB-K17/0794, CERT-BUND:CB-K17/0704, CERT-BUND:CB-K17/0659, CERT-BUND:CB-K17/0527, CERT-BUND:CB-K17/0477, CERT-BUND:CB-K17/0185, CERT-BUND:CB-K16/1995, DFN-CERT:DFN-CERT-2018-1764, DFN-CERT:DFN-CERT-2018-1070, DFN-CERT:DFN-CERT-2018-0077, DFN-CERT:DFN-CERT-2017-1925, DFN-CERT:DFN-CERT-2017-1692, DFN-CERT:DFN-CERT-2017-1327, DFN-CERT:DFN-CERT-2017-1204, DFN-CERT:DFN-CERT-2017-0988, DFN-CERT:DFN-CERT-2017-0814, DFN-CERT:DFN-CERT-2017-0723, DFN-CERT:DFN-CERT-2017-0673, DFN-CERT:DFN-CERT-2017-0532, DFN-CERT:DFN-CERT-2017-0489, DFN-CERT:DFN-CERT-2017-0189, DFN-CERT:DFN-CERT-2016-2108

## Scanner evidence for A291

The action above covers the following detailed scanner evidence.

Vendor references

CERT-BUND:WID-SEC-2025-0370, CERT-BUND:WID-SEC-2022-0673, CERT-BUND:CB-K22/0045, CERT-BUND:CB-K18/0066, CERT-BUND:CB-K17/2188, CERT-BUND:CB-K17/2013, CERT-BUND:CB-K17/1936, CERT-BUND:CB-K17/1854, CERT-BUND:CB-K17/1842, CERT-BUND:CB-K17/1768, CERT-BUND:CB-K17/1747, CERT-BUND:CB-K17/1622, CERT-BUND:CB-K17/1382, CERT-BUND:CB-K17/1279, CERT-BUND:CB-K17/1154, CERT-BUND:CB-K17/1023, DFN-CERT:DFN-CERT-2019-0358, DFN-CERT:DFN-CERT-2018-0077, DFN-CERT:DFN-CERT-2017-2290, DFN-CERT:DFN-CERT-2017-2104, DFN-CERT:DFN-CERT-2017-2021, DFN-

CERT:DFN-CERT-2017-1926, DFN-CERT:DFN-CERT-2017-1925, DFN-CERT:DFN-CERT-2017-1843, DFN-CERT:DFN-CERT-2017-1828, DFN-CERT:DFN-CERT-2017-1692, DFN-CERT:DFN-CERT-2017-1443, DFN-CERT:DFN-CERT-2017-1327, DFN-CERT:DFN-CERT-2017-1193, DFN-CERT:DFN-CERT-2017-1058

## Scanner evidence for A292

The action above covers the following detailed scanner evidence.

Vendor references

CERT-BUND:WID-SEC-2025-0370, CERT-BUND:CB-K18/0066, CERT-BUND:CB-K17/2013, CERT-BUND:CB-K17/1980, CERT-BUND:CB-K17/1936, CERT-BUND:CB-K17/1871, CERT-BUND:CB-K17/1854, CERT-BUND:CB-K17/1842, CERT-BUND:CB-K17/1768, CERT-BUND:CB-K17/1747, CERT-BUND:CB-K17/1622, CERT-BUND:CB-K17/1558, CERT-BUND:CB-K17/1382, CERT-BUND:CB-K17/1197, CERT-BUND:CB-K17/1177, CERT-BUND:CB-K17/1023, DFN-CERT:DFN-CERT-2019-0358, DFN-CERT:DFN-CERT-2018-0077, DFN-CERT:DFN-CERT-2017-2104, DFN-CERT:DFN-CERT-2017-2070, DFN-CERT:DFN-CERT-2017-2021, DFN-CERT:DFN-CERT-2017-1954, DFN-CERT:DFN-CERT-2017-1926, DFN-CERT:DFN-CERT-2017-1925, DFN-CERT:DFN-CERT-2017-1843, DFN-CERT:DFN-CERT-2017-1828, DFN-CERT:DFN-CERT-2017-1692, DFN-CERT:DFN-CERT-2017-1626, DFN-CERT:DFN-CERT-2017-1443, DFN-CERT:DFN-CERT-2017-1240, DFN-CERT:DFN-CERT-2017-1217, DFN-CERT:DFN-CERT-2017-1058

## Scanner evidence for A293

The action above covers the following detailed scanner evidence.

Vendor references

DFN-CERT:DFN-CERT-2011-0515, DFN-CERT:DFN-CERT-2011-0402, DFN-CERT:DFN-CERT-2011-0013, DFN-CERT:DFN-CERT-2011-0012, DFN-CERT:DFN-CERT-2011-0011, DFN-CERT:DFN-CERT-2010-1593

## Scanner evidence for A294

The action above covers the following detailed scanner evidence.

Vendor references

CERT-BUND:WID-SEC-2024-1055, CERT-BUND:CB-K17/0055, CERT-BUND:CB-K16/0684, CERT-BUND:CB-K16/0068, DFN-CERT:DFN-CERT-2017-0060, DFN-CERT:DFN-CERT-2016-0733, DFN-CERT:DFN-CERT-2016-0077

## Scanner evidence for A295

The action above covers the following detailed scanner evidence.

Vendor references

CERT-BUND:CB-K17/0054, CERT-BUND:CB-K16/1485, CERT-BUND:CB-K16/1107, CERT-BUND:CB-K16/0684, CERT-BUND:CB-K16/0449, CERT-BUND:CB-K16/0448, CERT-BUND:CB-K16/0397, DFN-CERT:DFN-CERT-2018-1828, DFN-CERT:DFN-CERT-2017-0059, DFN-CERT:DFN-CERT-2016-1574, DFN-CERT:DFN-CERT-2016-1174, DFN-CERT:DFN-CERT-2016-0733, DFN-CERT:DFN-CERT-2016-0488, DFN-CERT:DFN-CERT-2016-0486, DFN-CERT:DFN-CERT-2016-0437

## Scanner evidence for A296

The action above covers the following detailed scanner evidence.

Vendor references

CERT-BUND:WID-SEC-2024-1053, CERT-BUND:CB-K17/1725, CERT-BUND:CB-K17/0055, CERT-BUND:CB-K17/0054, CERT-BUND:CB-K16/1837, CERT-BUND:CB-K16/1487, CERT-BUND:CB-K16/1485, CERT-BUND:CB-K16/1221, CERT-BUND:CB-K16/0684, CERT-BUND:CB-K16/0577, DFN-CERT:DFN-CERT-2019-1408, DFN-CERT:DFN-CERT-2017-1807, DFN-CERT:DFN-CERT-2017-0060, DFN-CERT:DFN-CERT-2017-0059, DFN-CERT:DFN-CERT-2016-1943, DFN-CERT:DFN-CERT-2016-1576, DFN-CERT:DFN-CERT-2016-1574, DFN-CERT:DFN-

CERT-2016-1243, DFN-CERT:DFN-CERT-2016-0864, DFN-CERT:DFN-CERT-2016-0733, DFN-CERT:DFN-CERT-2016-0628

## Scanner evidence for A297

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2024-3195, CERT-BUND:WID-SEC-2024-1248, CERT-BUND:WID-SEC-2024-1082, CERT-BUND:WID-SEC-2024-0064, CERT-BUND:WID-SEC-2023-2679, CERT-BUND:WID-SEC-2023-2625, CERT-BUND:WID-SEC-2023-2240, CERT-BUND:WID-SEC-2023-1843, CERT-BUND:WID-SEC-2023-1819, DFN-CERT:DFN-CERT-2026-0097, DFN-CERT:DFN-CERT-2025-2802, DFN-CERT:DFN-CERT-2024-1260, DFN-CERT:DFN-CERT-2024-0491, DFN-CERT:DFN-CERT-2023-2792, DFN-CERT:DFN-CERT-2023-2179, DFN-CERT:DFN-CERT-2023-1961, DFN-CERT:DFN-CERT-2023-1920, DFN-CERT:DFN-CERT-2023-1845, DFN-CERT:DFN-CERT-2023-1773, DFN-CERT:DFN-CERT-2023-1665 |

## Scanner evidence for A298

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2012-1293, DFN-CERT:DFN-CERT-2009-1408 |

## Scanner evidence for A299

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2009-1064 |

## Scanner evidence for A300

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2025-1969, CERT-BUND:CB-K17/0814, DFN-CERT:DFN-CERT-2017-1382, DFN-CERT:DFN-CERT-2017-0837 |

## Scanner evidence for A301

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K17/1281, CERT-BUND:CB-K17/1129, DFN-CERT:DFN-CERT-2019-0726, DFN-CERT:DFN-CERT-2017-1329, DFN-CERT:DFN-CERT-2017-1168 |

## Scanner evidence for A305

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K15/0080, CERT-BUND:CB-K14/1505, CERT-BUND:CB-K14/0608, DFN-CERT:DFN-CERT-2015-0082, DFN-CERT:DFN-CERT-2014-1592, DFN-CERT:DFN-CERT-2014-0635, DFN-CERT:DFN-CERT-2013-1307, DFN-CERT:DFN-CERT-2012-1276, DFN-CERT:DFN-CERT-2012-1112, DFN-CERT:DFN-CERT-2012-0928, DFN-CERT:DFN-CERT-2012-0758, DFN-CERT:DFN-CERT-2012-0744, DFN-CERT:DFN-CERT-2012-0568, DFN-CERT:DFN-CERT-2012-0425, DFN-CERT:DFN-CERT-2012-0424, DFN-CERT:DFN-CERT-2012-0387, DFN-CERT:DFN-CERT-2012-0343, DFN-CERT:DFN-CERT-2012-0332, DFN-CERT:DFN-CERT-2012-0306, DFN-CERT:DFN-CERT-2012-0264, DFN-CERT:DFN-CERT-2012-0203, DFN-CERT:DFN-CERT-2012-0188 |

## Scanner evidence for A306

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K17/0054, CERT-BUND:CB-K16/1733, CERT-BUND:CB-K16/1315, CERT-BUND:CB-K16/0694, CERT-BUND:CB-K15/1591, CERT-BUND:CB-K15/1334, CERT-BUND:CB-K15/1194, CERT-BUND:CB-K15/0934, DFN-CERT:DFN-CERT-2018-1828, DFN-CERT:DFN-CERT-2017-0059, DFN-CERT:DFN-CERT-2016-1841, DFN-CERT:DFN-CERT-2016-1401, DFN-CERT:DFN-CERT-2016-0864, DFN-CERT:DFN-CERT-2016-0754, DFN-CERT:DFN-CERT-2015-1679, DFN-CERT:DFN-CERT-2015-1406, DFN-CERT:DFN-CERT-2015-1263, DFN-CERT:DFN-CERT-2015-0987 |

## Scanner evidence for A307

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K18/0066, CERT-BUND:CB-K17/0054, CERT-BUND:CB-K16/1733, CERT-BUND:CB-K16/1315, CERT-BUND:CB-K16/1107, CERT-BUND:CB-K16/1102, CERT-BUND:CB-K16/0694, CERT-BUND:CB-K16/0448, CERT-BUND:CB-K15/1696, CERT-BUND:CB-K15/1591, CERT-BUND:CB-K15/1561, CERT-BUND:CB-K15/1550, CERT-BUND:CB-K15/1510, CERT-BUND:CB-K15/1369, CERT-BUND:CB-K15/1334, CERT-BUND:CB-K15/1247, CERT-BUND:CB-K15/1212, CERT-BUND:CB-K15/1194, CERT-BUND:CB-K15/1188, CERT-BUND:CB-K15/1105, CERT-BUND:CB-K15/1103, DFN-CERT:DFN-CERT-2019-1408, DFN-CERT:DFN-CERT-2018-1828, DFN-CERT:DFN-CERT-2018-0077, DFN-CERT:DFN-CERT-2017-0059, DFN-CERT:DFN-CERT-2016-1841, DFN-CERT:DFN-CERT-2016-1401, DFN-CERT:DFN-CERT-2016-1174, DFN-CERT:DFN-CERT-2016-1168, DFN-CERT:DFN-CERT-2016-0754, DFN-CERT:DFN-CERT-2016-0486, DFN-CERT:DFN-CERT-2015-1794, DFN-CERT:DFN-CERT-2015-1679, DFN-CERT:DFN-CERT-2015-1644, DFN-CERT:DFN-CERT-2015-1632, DFN-CERT:DFN-CERT-2015-1591, DFN-CERT:DFN-CERT-2015-1443, DFN-CERT:DFN-CERT-2015-1406, DFN-CERT:DFN-CERT-2015-1263, DFN-CERT:DFN-CERT-2015-1259, DFN-CERT:DFN-CERT-2015-1252, DFN-CERT:DFN-CERT-2015-1239, DFN-CERT:DFN-CERT-2015-1161, DFN-CERT:DFN-CERT-2015-1159 |

## Scanner evidence for A308

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2010-1249, DFN-CERT:DFN-CERT-2010-1195, DFN-CERT:DFN-CERT-2010-1187 |

## Scanner evidence for A310

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2026-0180, CERT-BUND:WID-SEC-2025-1658, CERT-BUND:WID-SEC-2023-0431, CERT-BUND:CB-K17/1198, CERT-BUND:CB-K17/1196, CERT-BUND:CB-K16/1828, CERT-BUND:CB-K16/1438, CERT-BUND:CB-K16/1384, CERT-BUND:CB-K16/1102, CERT-BUND:CB-K16/0599, CERT-BUND:CB-K16/0156, CERT-BUND:CB-K15/1514, CERT-BUND:CB-K15/1358, CERT-BUND:CB-K15/1021, CERT-BUND:CB-K15/0972, CERT-BUND:CB-K15/0637, CERT-BUND:CB-K15/0590, CERT-BUND:CB-K15/0525, CERT-BUND:CB-K15/0393, CERT-BUND:CB-K15/0384, CERT-BUND:CB-K15/0287, CERT-BUND:CB-K15/0252, CERT-BUND:CB-K15/0246, CERT-BUND:CB-K15/0237, CERT-BUND:CB-K15/0118, CERT-BUND:CB-K15/0110, CERT-BUND:CB-K15/0108, CERT-BUND:CB-K15/0080, CERT-BUND:CB-K15/0078, CERT-BUND:CB-K15/0077, CERT-BUND:CB-K15/0075, CERT-BUND:CB-K14/1617, CERT-BUND:CB-K14/1581, CERT-BUND:CB-K14/1537, CERT-BUND:CB-K14/1479, CERT-BUND:CB-K14/1458, CERT-BUND:CB-K14/1342, CERT-BUND:CB-K14/1314, CERT-BUND:CB-K14/1313, CERT-BUND:CB-K14/1311, CERT-BUND:CB-K14/1304, CERT-BUND:CB-K14/1296, DFN-CERT:DFN-CERT-2017-1238, DFN-CERT:DFN-CERT-2017-1236, DFN-CERT:DFN- |

CERT-2016-1929, DFN-CERT:DFN-CERT-2016-1527, DFN-CERT:DFN-CERT-2016-1468, DFN-CERT:DFN-CERT-2016-1168, DFN-CERT:DFN-CERT-2016-0884, DFN-CERT:DFN-CERT-2016-0642, DFN-CERT:DFN-CERT-2016-0388, DFN-CERT:DFN-CERT-2016-0171, DFN-CERT:DFN-CERT-2015-1431, DFN-CERT:DFN-CERT-2015-1075, DFN-CERT:DFN-CERT-2015-1026, DFN-CERT:DFN-CERT-2015-0664, DFN-CERT:DFN-CERT-2015-0548, DFN-CERT:DFN-CERT-2015-0404, DFN-CERT:DFN-CERT-2015-0396, DFN-CERT:DFN-CERT-2015-0259, DFN-CERT:DFN-CERT-2015-0254, DFN-CERT:DFN-CERT-2015-0245, DFN-CERT:DFN-CERT-2015-0118, DFN-CERT:DFN-CERT-2015-0114, DFN-CERT:DFN-CERT-2015-0083, DFN-CERT:DFN-CERT-2015-0082, DFN-CERT:DFN-CERT-2015-0081, DFN-CERT:DFN-CERT-2015-0076, DFN-CERT:DFN-CERT-2014-1717, DFN-CERT:DFN-CERT-2014-1680, DFN-CERT:DFN-CERT-2014-1632, DFN-CERT:DFN-CERT-2014-1564, DFN-CERT:DFN-CERT-2014-1542, DFN-CERT:DFN-CERT-2014-1414, DFN-CERT:DFN-CERT-2014-1366, DFN-CERT:DFN-CERT-2014-1354

## Scanner evidence for A312

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2012-0320, DFN-CERT:DFN-CERT-2010-0984, DFN-CERT:DFN-CERT-2010-0491, DFN-CERT:DFN-CERT-2010-0462 |

## Scanner evidence for A313

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2012-0171, DFN-CERT:DFN-CERT-2011-1584, DFN-CERT:DFN-CERT-2011-1306, DFN-CERT:DFN-CERT-2011-1305, DFN-CERT:DFN-CERT-2011-1268, DFN-CERT:DFN-CERT-2011-1176, DFN-CERT:DFN-CERT-2010-0984, DFN-CERT:DFN-CERT-2010-0641, DFN-CERT:DFN-CERT-2010-0624, DFN-CERT:DFN-CERT-2010-0491, DFN-CERT:DFN-CERT-2010-0462, DFN-CERT:DFN-CERT-2010-0275 |

## Scanner evidence for A314

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2012-0171, DFN-CERT:DFN-CERT-2011-1584, DFN-CERT:DFN-CERT-2011-1306, DFN-CERT:DFN-CERT-2011-1305, DFN-CERT:DFN-CERT-2011-1117 |

## Scanner evidence for A316

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2013-1307, DFN-CERT:DFN-CERT-2013-0991 |

## Scanner evidence for A318

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2023-2979, CERT-BUND:WID-SEC-2022-1335, CERT-BUND:WID-SEC-2022-1228, CERT-BUND:WID-SEC-2022-0432, CERT-BUND:WID-SEC-2022-0302, CERT-BUND:CB-K22/0016, DFN-CERT:DFN-CERT-2022-0865, DFN-CERT:DFN-CERT-2022-0264, DFN-CERT:DFN-CERT-2022-0242, DFN-CERT:DFN-CERT-2022-0239, DFN-CERT:DFN-CERT-2022-0035 |

## Scanner evidence for A319

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2026-1194, CERT-BUND:WID-SEC-2026-0778, CERT-BUND:WID-SEC-2026-0489, CERT-BUND:WID-SEC-2026-0349, CERT-BUND:WID-SEC-2025-2212, DFN- |

CERT:DFN-CERT-2026-2045, DFN-CERT:DFN-CERT-2026-0955, DFN-CERT:DFN-CERT-2026-0392, DFN-CERT:DFN-CERT-2026-0218, DFN-CERT:DFN-CERT-2025-3384, DFN-CERT:DFN-CERT-2025-2768

## Scanner evidence for A321

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2022-2116, CERT-BUND:CB-K20/0788, DFN-CERT:DFN-CERT-2022-2639, DFN-CERT:DFN-CERT-2022-2638, DFN-CERT:DFN-CERT-2021-2373, DFN-CERT:DFN-CERT-2021-1645, DFN-CERT:DFN-CERT-2021-1453, DFN-CERT:DFN-CERT-2021-0380, DFN-CERT:DFN-CERT-2020-1910, DFN-CERT:DFN-CERT-2020-1732 |

## Scanner evidence for A322

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2010-0803 |

## Scanner evidence for A325

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:WID-SEC-2026-0180, CERT-BUND:CB-K21/0067, CERT-BUND:CB-K19/0812, CERT-BUND:CB-K16/1593, CERT-BUND:CB-K16/1552, CERT-BUND:CB-K16/0617, CERT-BUND:CB-K16/0599, CERT-BUND:CB-K16/0168, CERT-BUND:CB-K16/0121, CERT-BUND:CB-K16/0090, CERT-BUND:CB-K16/0030, CERT-BUND:CB-K15/1591, CERT-BUND:CB-K15/1550, CERT-BUND:CB-K15/1517, CERT-BUND:CB-K15/1464, CERT-BUND:CB-K15/1442, CERT-BUND:CB-K15/1334, CERT-BUND:CB-K15/1269, CERT-BUND:CB-K15/1136, CERT-BUND:CB-K15/1090, CERT-BUND:CB-K15/1059, CERT-BUND:CB-K15/1022, CERT-BUND:CB-K15/1015, CERT-BUND:CB-K15/0964, CERT-BUND:CB-K15/0932, CERT-BUND:CB-K15/0927, CERT-BUND:CB-K15/0926, CERT-BUND:CB-K15/0907, CERT-BUND:CB-K15/0901, CERT-BUND:CB-K15/0896, CERT-BUND:CB-K15/0877, CERT-BUND:CB-K15/0834, CERT-BUND:CB-K15/0802, CERT-BUND:CB-K15/0733, DFN-CERT:DFN-CERT-2023-2939, DFN-CERT:DFN-CERT-2021-0775, DFN-CERT:DFN-CERT-2020-1561, DFN-CERT:DFN-CERT-2020-1276, DFN-CERT:DFN-CERT-2016-1692, DFN-CERT:DFN-CERT-2016-1648, DFN-CERT:DFN-CERT-2016-0665, DFN-CERT:DFN-CERT-2016-0642, DFN-CERT:DFN-CERT-2016-0184, DFN-CERT:DFN-CERT-2016-0135, DFN-CERT:DFN-CERT-2016-0101, DFN-CERT:DFN-CERT-2016-0035, DFN-CERT:DFN-CERT-2015-1679, DFN-CERT:DFN-CERT-2015-1632, DFN-CERT:DFN-CERT-2015-1608, DFN-CERT:DFN-CERT-2015-1542, DFN-CERT:DFN-CERT-2015-1518, DFN-CERT:DFN-CERT-2015-1406, DFN-CERT:DFN-CERT-2015-1341, DFN-CERT:DFN-CERT-2015-1194, DFN-CERT:DFN-CERT-2015-1144, DFN-CERT:DFN-CERT-2015-1113, DFN-CERT:DFN-CERT-2015-1078, DFN-CERT:DFN-CERT-2015-1067, DFN-CERT:DFN-CERT-2015-1016, DFN-CERT:DFN-CERT-2015-0980, DFN-CERT:DFN-CERT-2015-0977, DFN-CERT:DFN-CERT-2015-0976, DFN-CERT:DFN-CERT-2015-0960, DFN-CERT:DFN-CERT-2015-0956, DFN-CERT:DFN-CERT-2015-0944, DFN-CERT:DFN-CERT-2015-0925, DFN-CERT:DFN-CERT-2015-0879, DFN-CERT:DFN-CERT-2015-0844, DFN-CERT:DFN-CERT-2015-0737 |

## Scanner evidence for A326

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2012-0618, DFN-CERT:DFN-CERT-2011-0700, DFN-CERT:DFN-CERT-2010-1647, DFN-CERT:DFN-CERT-2010-0730, DFN-CERT:DFN-CERT-2010-0446, DFN-CERT:DFN-CERT-2010-0273, DFN-CERT:DFN-CERT-2009-1809, DFN-CERT:DFN-CERT-2009-1755, DFN-CERT:DFN-CERT-2009-1725, DFN-CERT:DFN-CERT-2009-1623, DFN- |

| | |
|---|---|
| | CERT:DFN-CERT-2009-1603, DFN-CERT:DFN-CERT-2009-1602, DFN-CERT:DFN-CERT-2009-1507, DFN-CERT:DFN-CERT-2009-1340, DFN-CERT:DFN-CERT-2009-1326 |

## Scanner evidence for A327

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2010-0984, DFN-CERT:DFN-CERT-2010-0682, DFN-CERT:DFN-CERT-2010-0681, DFN-CERT:DFN-CERT-2010-0680 |

## Scanner evidence for A329

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | DFN-CERT:DFN-CERT-2012-1276 |

## Scanner evidence for A330

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K15/1514, CERT-BUND:CB-K14/0632, DFN-CERT:DFN-CERT-2014-0658 |

## Scanner evidence for A331

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K16/0944, CERT-BUND:CB-K14/1167, DFN-CERT:DFN-CERT-2016-1004, DFN-CERT:DFN-CERT-2014-1219 |

## Scanner evidence for A332

The action above covers the following detailed scanner evidence.

| | |
|---|---|
| Vendor references | CERT-BUND:CB-K15/1514, DFN-CERT:DFN-CERT-2021-0770, DFN-CERT:DFN-CERT-2012-0852, DFN-CERT:DFN-CERT-2010-0803, DFN-CERT:DFN-CERT-2009-1232, DFN-CERT:DFN-CERT-2009-1129 |