Vulnerability Prioritization Report

Findings from one Nessus export, grouped into the priority bands below.

Generated
2026-09-13T18:35:50Z

Scan date
2026-08-28T06:00:00

Assessment
Assessment type: Automated network vulnerability assessment (Tenable Nessus, credentialed where noted), prioritized against CISA KEV exploitation data, with EPSS exploit-likelihood data reported alongside.

Report ID
20260913T183550Z

Confidentiality
Confidential — contains sensitive security information

15	23	3	6
Distinct issues	Raw scan occurrences (incl. per-port duplicates)	Hosts scanned	**Past CISA KEV target date**

Executive summary

The scan reports findings matched to known-exploited vulnerabilities, requiring prioritized remediation, including items past their CISA KEV target dates.

Recommended priority action (A1): Vendor patch / advisory for 2 assets across 2 findings. Covers 1 CISA KEV-listed finding, including 1 with known ransomware campaign use.

Business impact themes

- Unpatched software can leave known weaknesses available to attackers.
- Weak certificate or cryptographic settings can reduce confidentiality or trust in affected services.

Assessment basis

6 of 15 distinct issues are listed in CISA's KEV catalog as known exploited, across 3 hosts. 6 are already past their CISA KEV target date. CISA records known use of 5 of those in ransomware campaigns. These come first, ahead of anything ranked on CVSS alone, because recorded exploitation outweighs theoretical severity. Review the detailed guidance and its provenance below before selecting and verifying remediation.

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.

5 of 15 retained issues have no CVE; CVE-based KEV and EPSS checks cannot assess those issues.

6	3	5
CISA known exploited	Hosts affected	Ransomware-linked

> Every issue below is listed in CISA's Known Exploited Vulnerabilities catalog: CISA records each of these CVEs as known to have been exploited. Remediate them ahead of anything ranked on CVSS alone. The CISA KEV target dates shown are remediation deadlines that BOD 26-04 makes binding on U.S. Federal Civilian Executive Branch agencies; for other organizations they are prioritization guidance, not an obligation. Issues marked as ransomware-linked are CVEs CISA records as used in known ransomware campaigns; that record does not establish a compromise or predict the impact for this environment.

10 remediation actions address all 12 prioritized findings, including every KEV-listed issue. 2 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: 12 prioritized findings are covered by 10 actions.

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

#1 Netlogon Elevation of Privilege (Zerologon) 1,761 days past CISA target Ransomware-linked

CVE-2020-1472, CVSS 10.0, on 1 host: 10.20.30.11 (dc01.corp.example.test).

Past CISA KEV target date by 1,761 days (CVE-2020-1472 target 2021-11-17)

#2 Apache Log4j 2.x < 2.15.0 Remote Code Execution 1,724 days past CISA target Ransomware-linked

CVE-2021-44228, CVSS 10.0, on 1 host: 10.20.30.42 (app02.corp.example.test).

Past CISA KEV target date by 1,724 days (CVE-2021-44228 target 2021-12-24)

#3 Microsoft Windows Remote Desktop Services RCE (BlueKeep) 1,761 days past CISA target Ransomware-linked

CVE-2019-0708, CVSS 9.8, on 1 host: 10.20.30.11 (dc01.corp.example.test).

Past CISA KEV target date by 1,761 days (CVE-2019-0708 target 2021-11-17)

#4 Windows Print Spooler RCE (PrintNightmare) 1,881 days past CISA target Ransomware-linked

CVE-2021-34527, CVSS 8.8, on 2 hosts: 10.20.30.11 (dc01.corp.example.test), 10.20.30.77 (ws14.corp.example.test).

Past CISA KEV target date by 1,881 days (CVE-2021-34527 target 2021-07-20)

#5 MS17-010: Security Update for Microsoft Windows SMB Server 1,761 days past CISA target Ransomware-linked

CVE-2017-0144, CVSS 8.1, on 2 hosts: 10.20.30.11 (dc01.corp.example.test), 10.20.30.77 (ws14.corp.example.test).

Past CISA KEV target date by 1,761 days (CVE-2017-0144 target 2021-11-17)

#6 OpenSSL Heartbeat Information Disclosure (Heartbleed) 1,612 days past CISA target

CVE-2014-0160, CVSS 7.5, on 1 host: 10.20.30.42 (app02.corp.example.test).

> **Past CISA KEV target date by 1,612 days (CVE-2014-0160 target 2022-04-15)**

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	5
Band 2	KEV	in CISA KEV (CISA records these CVEs as known to have been exploited)	1
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 Nessus severity 2 or above	4
Band 5	no CVE, non-trivial severity	no CVE, but Nessus severity at or above 2	2
Band 6	low or informational	any finding the bands above do not match	3

Scanner	Unknown
Scanner version	Unknown
Policy	Basic Network Scan
Plugin feed date	Unknown
Scan window start	2026-08-28T06:00:00
Scan window end	2026-08-28T06:14:00
Credentialed	Unknown
Targets	Unknown

3
Hosts scanned

Unknown
Credential coverage

0
Hosts where patch assessment failed

0
Hosts missing a hostname

0
Hosts missing OS detail

10
Retained occurrences missing a CVE

6
Retained occurrences missing CVSS

5
Retained occurrences with no actionable solution (no text, or a placeholder such as "n/a")

5
Retained occurrences at informational severity

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

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.
- Scanner product name, scanner version, and plugin feed date, which this export does not record in a form this report can read.

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.

A1 Vendor patch / advisory on 2 assets — resolves 3 instances across 2 findings

Apply the MS17-010 security update.

> Affected service: 445/tcp (cifs).

Version target	No version stated; apply the referenced advisory (MS17-010)
KEV / ransomware	Covers 1 CISA KEV-listed finding, including 1 with known ransomware campaign use.
Highest EPSS (covered findings)	94.5% probability, >99.9% percentile
Guidance source	Scanner-supplied — the wording above is the scanner's own solution text.
Validation	Rescan with plugins 34477, 200101 after the change; they should stop reporting on all 2 affected assets.

A2 Vendor patch / advisory on 2 assets — resolves 2 instances across 1 finding

Apply the July 2021 out-of-band security update.

> Affected service: 445/tcp (cifs).

KEV / ransomware	Covers 1 CISA KEV-listed finding, including 1 with known ransomware campaign use.
Highest EPSS (covered findings)	52.3% probability, 95.3% percentile
Guidance source	Scanner-supplied — the wording above is the scanner's own solution text.
Validation	Rescan with plugin 151478 after the change; it should stop reporting on all 2 affected assets.

A3 Vendor patch / advisory on 1 asset — resolves 1 instance across 1 finding

Apply the August 2020 security update and enforce secure RPC.

> Affected service: 445/tcp (cifs).

KEV / ransomware	Covers 1 CISA KEV-listed finding, including 1 with known ransomware campaign use.
Highest EPSS (covered findings)	76.3% probability, 98.7% percentile
Guidance source	Scanner-supplied — the wording above is the scanner's own solution text.
Validation	Rescan with plugin 140770 after the change; it should stop reporting on the affected asset.

A4 Vendor patch / advisory on 1 asset — resolves 1 instance across 1 finding

Apply the May 2019 security update.

> Affected service: 3389/tcp (msrdp).

KEV / ransomware	Covers 1 CISA KEV-listed finding, including 1 with known ransomware campaign use.
Highest EPSS (covered findings)	88.3% probability, 99.9% percentile
Guidance source	Scanner-supplied — the wording above is the scanner's own solution text.
Validation	Rescan with plugin 125313 after the change; it should stop reporting on the affected asset.

A5 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Upgrade Log4j to 2.17.1 or later.

> Affected service: 8080/tcp (http).

Version target	Minimum fixed version stated by the scanner (an open range — a later version may be required): Log4j 2.17.1
KEV / ransomware	Covers 1 CISA KEV-listed finding, including 1 with known ransomware campaign use.
Highest EPSS (covered findings)	97.4% probability, 100% percentile
Guidance source	Scanner-supplied — the wording above is the scanner's own solution text.
Validation	Rescan with plugin 155999 after the change; it should stop reporting on the affected asset.

A6 Version upgrade on 1 asset — resolves 1 instance across 1 finding

Upgrade to OpenSSL 1.0.1g or later and reissue certificates.

> Affected service: 443/tcp (https).

Version target	Minimum fixed version stated by the scanner (an open range — a later version may be required): OpenSSL 1.0.1g
KEV / ransomware	Covers 1 CISA KEV-listed finding.
Highest EPSS (covered findings)	41.2% probability, 93.1% percentile
Guidance source	Scanner-supplied — the wording above is the scanner's own solution text.
Validation	Rescan with plugin 73412 after the change; it should stop reporting on the affected asset.

A7 Certificate / cryptographic configuration on 3 assets — resolves 3 instances across 2 findings

Reconfigure the service to disable 3DES cipher suites.

> Affected service: 443/tcp (https).

Highest EPSS (covered findings)	3.5% probability, 68.7% percentile
Guidance source	Scanner-supplied — the wording above is the scanner's own solution text.
Validation	Rescan with plugins 94437, 200102 after the change; they should stop reporting on all 3 affected assets.

A8 Certificate / cryptographic configuration on 1 asset — resolves 1 instance across 1 finding

Reconfigure the service to disable RC4.

> Affected service: 443/tcp (https).

Highest EPSS (covered findings)	covered findings carry a CVE, but none is scored in the loaded feed
Guidance source	Scanner-supplied — the wording above is the scanner's own solution text.
Validation	Rescan with plugin 65821 after the change; it should stop reporting on the affected asset.

A9 Certificate / cryptographic configuration on 2 assets — resolves 2 instances across 1 finding

Install a certificate signed by a recognized authority.

> Affected service: 443/tcp (https).

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 57582 after the change; it should stop reporting on all 2 affected assets.

A10 Certificate / cryptographic configuration on 1 asset — resolves 2 instances across 1 finding

Reconfigure the affected application, if possible, to avoid the use of medium strength ciphers.

> Covers 2 distinct services (443/tcp (https), 8443/tcp (https)). 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 42873 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.

A11 No scanner-supplied solution — manual review: covers 5 instances across 2 findings on 3 assets.

A12 Scanner-stated remediation, not categorized: covers 1 instance across 1 finding on 1 asset; see plugin 200103 in the scan.

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 1** KEV + ransomware **Act now**	**Netlogon Elevation of Privilege (Zerologon)** Plugin 140770 CVE-2020-1472 KEV: Past CISA KEV target date by 1,761 days (CVE-2020-1472 target 2021-11-17) — EPSS: 76.3% probability, 98.7% percentile — CVSS: 10.0 (v3.x) — Exploit available: Unknown Technical risk (Nessus synopsis) The remote Windows domain controller is affected by an EoP vulnerability. See appendix	1	1

#	Priority / band	Issue	Hosts	Instances
2	**Band 1** KEV + ransomware **Act now**	**Apache Log4j 2.x < 2.15.0 Remote Code Execution** Plugin 155999 CVE-2021-44228 KEV: Past CISA KEV target date by 1,724 days (CVE-2021-44228 target 2021-12-24) — EPSS: 97.4% probability, 100% percentile — CVSS: 10.0 (v3.x) — Exploit available: Unknown Technical risk (Nessus synopsis) The remote host runs a version of Log4j vulnerable to JNDI injection. See appendix	1	1
3	**Band 1** KEV + ransomware **Act now**	**Microsoft Windows Remote Desktop Services RCE (BlueKeep)** Plugin 125313 CVE-2019-0708 KEV: Past CISA KEV target date by 1,761 days (CVE-2019-0708 target 2021-11-17) — EPSS: 88.3% probability, 99.9% percentile — CVSS: 9.8 (v3.x) — Exploit available: Unknown Technical risk (Nessus synopsis) The remote host is affected by a pre-authentication RCE in RDP. See appendix	1	1
4	**Band 1** KEV + ransomware **Act now**	**Windows Print Spooler RCE (PrintNightmare)** Plugin 151478 CVE-2021-34527 KEV: Past CISA KEV target date by 1,881 days (CVE-2021-34527 target 2021-07-20) — EPSS: 52.3% probability, 95.3% percentile — CVSS: 8.8 (v3.x) — Exploit available: Unknown Technical risk (Nessus synopsis) The remote host is affected by a Print Spooler remote code execution flaw. See appendix	2	2
5	**Band 1** KEV + ransomware **Act now**	**MS17-010: Security Update for Microsoft Windows SMB Server** Plugin 34477 CVE-2017-0144 KEV: Past CISA KEV target date by 1,761 days (CVE-2017-0144 target 2021-11-17) — EPSS: 94.5% probability, >99.9% percentile — CVSS: 8.1 (v3.x) — Exploit available: Unknown Technical risk (Nessus synopsis) The remote Windows host is affected by remote code execution vulnerabilities in SMBv1. See appendix	2	2
6	**Band 2** KEV **Act now**	**OpenSSL Heartbeat Information Disclosure (Heartbleed)** Plugin 73412 CVE-2014-0160 KEV: Past CISA KEV target date by 1,612 days (CVE-2014-0160 target 2022-04-15) — EPSS: 41.2% probability, 93.1% percentile — CVSS: 7.5 (v3.x) — Exploit available: Unknown Technical risk (Nessus synopsis) The remote service may disclose memory contents to unauthenticated clients. See appendix	1	1
7	**Band 4** has CVE, non-trivial severity **Schedule**	**Microsoft Windows SMBv1 Multiple Remote Code Execution Vulnerabilities** Plugin 200101 CVE-2017-0143, CVE-2017-0146 KEV: No KEV match in the catalog snapshot used — EPSS: 62.3% probability, 96.9% percentile — CVSS: 8.1 (v3.x) — Exploit available: Unknown Technical risk (Nessus synopsis) The remote Windows host is affected by multiple remote code execution vulnerabilities in SMBv1. See appendix	1	1

#	Priority / band	Issue	Hosts	Instances
8	**Band 4** has CVE, non-trivial severity **Schedule**	**SSL/TLS Birthday attack on 64-bit block ciphers (SWEET32)** Plugin 94437 CVE-2016-2183 KEV: No KEV match in the catalog snapshot used — EPSS: 3.5% probability, 68.7% percentile — CVSS: 7.5 (v3.x) — Exploit available: Unknown Technical risk (Nessus synopsis) The remote service supports 3DES cipher suites with 64-bit block size. See appendix	2	2
9	**Band 4** has CVE, non-trivial severity **Schedule**	**SSL/TLS 3DES Cipher Suite Vulnerability (Alternate Detection Method)** Plugin 200102 CVE-2016-2183 KEV: No KEV match in the catalog snapshot used — EPSS: 3.5% probability, 68.7% percentile — CVSS: 7.5 (v3.x) — Exploit available: Unknown Technical risk (Nessus synopsis) The remote service supports 3DES cipher suites with 64-bit block size, detected via an alternate check. See appendix	1	1
10	**Band 4** has CVE, non-trivial severity **Schedule**	**SSL RC4 Cipher Suites Supported (Bar Mitzvah)** Plugin 65821 CVE-2015-2808 KEV: No KEV match in the catalog snapshot used — EPSS: no scored CVE for this issue — CVSS: 5.9 (v3.x) — Exploit available: Unknown Technical risk (Nessus synopsis) The remote service supports RC4 cipher suites. See appendix	1	1
11	**Band 5** no CVE, non-trivial severity **Schedule**	**SSL Medium Strength Cipher Suites Supported** Plugin 42873 — KEV: No CVE to check against CISA KEV — EPSS: no scored CVE for this issue — CVSS: 6.8 (v3.x) — Exploit available: Unknown Technical risk (Nessus synopsis) The remote service supports the use of medium strength SSL ciphers. See appendix	1	2
12	**Band 5** no CVE, non-trivial severity **Schedule**	**SSL Self-Signed Certificate** Plugin 57582 — KEV: No CVE to check against CISA KEV — EPSS: no scored CVE for this issue — CVSS: 6.5 (v3.x) — Exploit available: Unknown Technical risk (Nessus synopsis) The SSL certificate chain terminates in a self-signed certificate. See appendix	2	2

Technical appendix

#1 Netlogon Elevation of Privilege (Zerologon)

Band 1 KEV + ransomware Plugin 140770

Past CISA KEV target date by 1,761 days (CVE-2020-1472 target 2021-11-17)

CVEs	CVE-2020-1472
CVSS base score	10.0
CISA KEV target date	2021-11-17 **1,761 days past target**
Remediation	Addressed by remediation action A3
Affected hosts (1)	**10.20.30.11** dc01.corp.example.test 445/tcp (cifs)
Scoring rationale	Band 1 (KEV + ransomware): in CISA KEV, with CISA-recorded use in known ransomware campaigns. CVE-2020-1472 added to CISA KEV 2021-11-03; CISA KEV target date 2021-11-17; known ransomware campaign use. CVSS 10.0. Nessus severity 4.
Rank position	Position 1 of 5 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: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

#2 Apache Log4j 2.x < 2.15.0 Remote Code Execution

Band 1 KEV + ransomware Plugin 155999

Past CISA KEV target date by 1,724 days (CVE-2021-44228 target 2021-12-24)

CVEs	CVE-2021-44228
CVSS base score	10.0
CISA KEV target date	2021-12-24 **1,724 days past target**
Remediation	Addressed by remediation action A5
Affected hosts (1)	**10.20.30.42** app02.corp.example.test 8080/tcp (http)
Scoring rationale	Band 1 (KEV + ransomware): in CISA KEV, with CISA-recorded use in known ransomware campaigns. CVE-2021-44228 added to CISA KEV 2021-12-10; CISA KEV target date 2021-12-24; known ransomware campaign use. CVSS 10.0. Nessus severity 4.
Rank position	Position 2 of 5 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: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

#3 Microsoft Windows Remote Desktop Services RCE (BlueKeep)

Band 1 KEV + ransomware Plugin 125313

Past CISA KEV target date by 1,761 days (CVE-2019-0708 target 2021-11-17)

CVEs	CVE-2019-0708
CVSS base score	9.8
CISA KEV target date	2021-11-17 **1,761 days past target**
Remediation	Addressed by remediation action A4
Affected hosts (1)	**10.20.30.11** dc01.corp.example.test 3389/tcp (msrdp)
Scoring rationale	Band 1 (KEV + ransomware): in CISA KEV, with CISA-recorded use in known ransomware campaigns. CVE-2019-0708 added to CISA KEV 2021-11-03; CISA KEV target date 2021-11-17; known ransomware campaign use. CVSS 9.8. Nessus severity 4.
Rank position	Position 3 of 5 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

#4 Windows Print Spooler RCE (PrintNightmare)

Band 1 KEV + ransomware Plugin 151478

Past CISA KEV target date by 1,881 days (CVE-2021-34527 target 2021-07-20)

CVEs	CVE-2021-34527
CVSS base score	8.8
CISA KEV target date	2021-07-20 **1,881 days past target**
Remediation	Addressed by remediation action A2
Affected hosts (2)	**10.20.30.11** dc01.corp.example.test 445/tcp (cifs) **10.20.30.77** ws14.corp.example.test 445/tcp (cifs)
Scoring rationale	Band 1 (KEV + ransomware): in CISA KEV, with CISA-recorded use in known ransomware campaigns. CVE-2021-34527 added to CISA KEV 2021-07-08; CISA KEV target date 2021-07-20; known ransomware campaign use. CVSS 8.8. Nessus severity 3.
Rank position	Position 4 of 5 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

#5 MS17-010: Security Update for Microsoft Windows SMB Server

Band 1 KEV + ransomware Plugin 34477

Past CISA KEV target date by 1,761 days (CVE-2017-0144 target 2021-11-17)

CVEs	CVE-2017-0144
CVSS base score	8.1
CISA KEV target date	2021-11-17 **1,761 days past target**
Remediation	Addressed by remediation action A1
Affected hosts (2)	**10.20.30.11** dc01.corp.example.test 445/tcp (cifs) **10.20.30.77** ws14.corp.example.test 445/tcp (cifs)
Scoring rationale	Band 1 (KEV + ransomware): in CISA KEV, with CISA-recorded use in known ransomware campaigns. CVE-2017-0144 added to CISA KEV 2021-11-03; CISA KEV target date 2021-11-17; known ransomware campaign use. CVSS 8.1. Nessus severity 4.
Rank position	Position 5 of 5 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:H/A:H — Attack vector: Network — Privileges required: None — User interaction: None — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

#6 OpenSSL Heartbeat Information Disclosure (Heartbleed)

Band 2 KEV Plugin 73412

Past CISA KEV target date by 1,612 days (CVE-2014-0160 target 2022-04-15)

CVEs	CVE-2014-0160
CVSS base score	7.5
CISA KEV target date	2022-04-15 **1,612 days past target**
Remediation	Addressed by remediation action A6
Affected hosts (1)	**10.20.30.42** app02.corp.example.test 443/tcp (https)
Scoring rationale	Band 2 (KEV): in CISA KEV (CISA records these CVEs as known to have been exploited). CVE-2014-0160 added to CISA KEV 2022-03-25; CISA KEV target date 2022-04-15. CVSS 7.5. Nessus severity 3. Ranked above Microsoft Windows SMBv1 Multiple Remote Code Execution Vulnerabilities (CVSS 8.1, no KEV match) because CISA-recorded exploitation outweighs CVSS.
Rank position	Position 1 of 1 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

#7 Microsoft Windows SMBv1 Multiple Remote Code Execution Vulnerabilities

Band 4 has CVE, non-trivial severity Plugin 200101

CVEs	CVE-2017-0143, CVE-2017-0146
CVSS base score	8.1
Remediation	Addressed by remediation action A1
Affected hosts (1)	**10.20.30.11** dc01.corp.example.test 445/tcp (cifs)
Scoring rationale	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 Nessus severity 2 or above. CVE-2017-0143, CVE-2017-0146 did not match the CISA KEV catalog snapshot used for this report. CVSS 8.1. Nessus severity 4.
Rank position	Position 1 of 4 within band, ordered by CVSS descending, then severity rating, then finding identifier.

CVSS vector: Unknown — Attack vector: Unknown — Privileges required: Unknown — User interaction: Unknown — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

#8 SSL/TLS Birthday attack on 64-bit block ciphers (SWEET32)

Band 4 has CVE, non-trivial severity Plugin 94437

CVEs	CVE-2016-2183
CVSS base score	7.5
Remediation	Addressed by remediation action A7
Affected hosts (2)	**10.20.30.42** app02.corp.example.test 443/tcp (https) **10.20.30.77** ws14.corp.example.test 443/tcp (https)
Scoring rationale	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 Nessus severity 2 or above. CVE-2016-2183 did not match the CISA KEV catalog snapshot used for this report. CVSS 7.5. Nessus severity 2.
Rank position	Position 2 of 4 within band, ordered by CVSS descending, then severity rating, then finding identifier.

CVSS vector: Unknown — Attack vector: Unknown — Privileges required: Unknown — User interaction: Unknown — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

#9 SSL/TLS 3DES Cipher Suite Vulnerability (Alternate Detection Method)

Band 4 has CVE, non-trivial severity Plugin 200102

CVEs	CVE-2016-2183
CVSS base score	7.5
Remediation	Addressed by remediation action A7
Affected hosts (1)	**10.20.30.11** dc01.corp.example.test 443/tcp (https)
Scoring rationale	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 Nessus severity 2 or above. CVE-2016-2183 did not match the CISA KEV catalog snapshot used for this report. CVSS 7.5. Nessus severity 2.
Rank position	Position 3 of 4 within band, ordered by CVSS descending, then severity rating, then finding identifier.

CVSS vector: Unknown — Attack vector: Unknown — Privileges required: Unknown — User interaction: Unknown — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

#10 SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Band 4 has CVE, non-trivial severity Plugin 65821

CVEs	CVE-2015-2808
CVSS base score	5.9
Remediation	Addressed by remediation action A8
Affected hosts (1)	**10.20.30.42** app02.corp.example.test 443/tcp (https)
Scoring rationale	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 Nessus severity 2 or above. CVE-2015-2808 did not match the CISA KEV catalog snapshot used for this report. CVSS 5.9. Nessus severity 2. Ranked above SSL Medium Strength Cipher Suites Supported (CVSS 6.8, no KEV match) because a known CVE outweighs a higher-CVSS finding that has no CVE.
Rank position	Position 4 of 4 within band, ordered by CVSS descending, then severity rating, then finding identifier.

CVSS vector: Unknown — Attack vector: Unknown — Privileges required: Unknown — User interaction: Unknown — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

#11 SSL Medium Strength Cipher Suites Supported

Band 5 no CVE, non-trivial severity Plugin 42873

CVEs	—
CVSS base score	6.8
Remediation	Addressed by remediation action A10
Affected hosts (1)	**10.20.30.42** app02.corp.example.test 443/tcp (https), 8443/tcp (https)
Scoring rationale	Band 5 (no CVE, non-trivial severity): no CVE, but Nessus severity at or above 2. CVSS 6.8. Nessus severity 2.
Rank position	Position 1 of 2 within band, ordered by CVSS descending, then severity rating, then finding identifier.

CVSS vector: Unknown — Attack vector: Unknown — Privileges required: Unknown — User interaction: Unknown — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

#12 SSL Self-Signed Certificate

Band 5 no CVE, non-trivial severity Plugin 57582

CVEs	—
CVSS base score	6.5
Remediation	Addressed by remediation action A9
Affected hosts (2)	**10.20.30.11** dc01.corp.example.test 443/tcp (https) **10.20.30.42** app02.corp.example.test 443/tcp (https)
Scoring rationale	Band 5 (no CVE, non-trivial severity): no CVE, but Nessus severity at or above 2. CVSS 6.5. Nessus severity 2.
Rank position	Position 2 of 2 within band, ordered by CVSS descending, then severity rating, then finding identifier.

CVSS vector: Unknown — Attack vector: Unknown — Privileges required: Unknown — User interaction: Unknown — Exploitability ease: Unknown — Internet exposure: Not assessed — Asset criticality: Not assessed

Low or informational findings (reference only)

3 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
13	Deprecated Service Component Reported (End-of-Life)	200103	1	A12
14	Traceroute Information	10287	2	A11
15	Nessus SYN scanner	11219	3	A11

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 Tenable Nessus 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 Nessus severity 2 or above. Band 5 (no CVE, non-trivial severity): no CVE, but Nessus severity at or above 2. 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.