

Vulnerability remediation report for Northwind Clinics (demo)

PREPARED FOR	PREPARED BY	SCAN DATE	STATUS
Northwind Clinics (demo)	Varaxon Technologies	2026-08-28	Complete

Executive summary

Several serious issues need prompt action, starting with Windows servers and a web server that match CISA's list of known exploited vulnerabilities.

This review covers the vulnerability scan of 3 hosts, taken on 2026-08-28. The scanner reported 15 distinct findings across 3 hosts. A scan is a point-in-time view from one vantage point, so it shows what was visible at that time. It does not show that the systems are free of other weaknesses.

7 findings match CISA's Known Exploited Vulnerabilities (KEV) catalog, a list CISA keeps of flaws it records as exploited. 6 of these have known ransomware campaign use recorded by CISA. They sit on the Windows servers and on app02.corp.example.test, and they come first in this plan.

Work is grouped into campaigns in priority order. Most of the Windows work fits in one visit. Each change includes a rescan to confirm it worked. Several changes need restarts, so those should be planned in advance.

Key points

- All KEV matches fall in the top two priority bands and need action first.
- The Windows update work on the Windows servers addresses the most serious items.
- The scan does not name the software behind the HTTPS services, so some encryption fixes need checks first.
- The export does not state whether the scan used logged-in access, so it may have missed items visible only to a logged-in check.
- Some findings have no solution text in the scan, so a technician must review them before any change.

Decisions for leadership

- Approve a maintenance window with restarts for the Windows servers and app02.corp.example.test as soon as it can be scheduled.
- Approve a short outage window for restarting the HTTPS services on the affected hosts.
- Approve scheduled work to replace the self-signed certificates with certificates from a recognized certificate authority.
- Decide whether to accept the lower-priority risks until the next review, and record that decision.

Findings at a glance

Findings by priority band

● Band 1	KEV + ransomware		6
● Band 2	KEV		1
● Band 3	urgent CVSS, no KEV match		0
● Band 4	has CVE, non-trivial severity		3
● Band 5	no CVE, non-trivial severity		2
● Band 6	low or informational		3

3

hosts with findings

3

hosts scanned

15

distinct findings

7

known exploited
(KEV)

12

remediation actions

Remediation plan

Band 1 Apply the Windows security updates on the Windows servers

Actions 1, 2, 3, 4

These findings sit on the Windows servers, and several match CISA's KEV catalog with recorded ransomware use. This is the first work to complete. The scanner names Microsoft security updates as the fix but does not give the exact build, so each host's current build needs checking first.

Steps for the technician

1. Check the installed Windows edition and build on each Windows server, and record them.
2. Confirm which of the named Microsoft security updates are already installed, and note any that are missing.
3. Install the MS17-010 update and the July 2021 out-of-band update on the Windows servers that need them.
4. On dc01.corp.example.test, install the August 2020 update and then enforce secure RPC for Netlogon. Install the May 2019 Remote Desktop update on dc01.corp.example.test as well.
5. Restart each server when its update requires a restart, inside the planned change window.
6. Verify by rescanning the Windows plugins named in the scanner output and confirming they no longer report on the affected hosts.

These updates need restarts, and the scan does not say which ones require them. Plan downtime for the Windows servers. Enforcing secure RPC on dc01.corp.example.test can stop devices that use Netlogon from connecting, so test before enforcing.

The scanner did not name a KB number or Windows build for these fixes, so the fix cannot be confirmed from the scan alone. Check each host against the vendor's record for its build.

Band 1 Upgrade the Log4j library on app02.corp.example.test

Actions 5

The scanner reported a remote code execution flaw in the Log4j logging library. CISA lists it in KEV with recorded ransomware use. The application that bundles Log4j is not named in the scan, so the first job is finding it.

Steps for the technician

1. Find the application on app02.corp.example.test that bundles Log4j, and record the installed Log4j version.
2. Check the vendor's upgrade path for that application, and prefer the vendor's supported update.
3. Upgrade Log4j to 2.17.1 or later, which is the minimum the scanner states. Check whether a later release is needed.
4. Restart the application so it loads the new library.
5. Verify by rescanning the Log4j plugin on app02.corp.example.test at TCP port 8080 and confirming it no longer reports.

Restarting the application interrupts the service for its users. The scanner gives 2.17.1 only as a minimum, so check the installed version again after the change.

Band 2 Upgrade OpenSSL on app02.corp.example.test and replace its certificates and keys

Actions 6

The scanner reported an information disclosure flaw in OpenSSL, known as Heartbleed. CISA lists it in KEV. The scanner advises reissuing certificates and keys after the upgrade, so plan that work with the upgrade itself.

Steps for the technician

1. Confirm the installed OpenSSL version and the operating system on app02.corp.example.test.
2. If the host uses a Linux distribution package, check that distribution's fixed build, which can differ from the upstream version.
3. Upgrade OpenSSL to 1.0.1g or later, or to the distribution's fixed build.
4. Reissue the certificates and keys on the host, and retire the old ones.
5. Restart the services that use OpenSSL.
6. Verify by rescanning the OpenSSL plugin on app02.corp.example.test at TCP port 443 and confirming it no longer reports.

The scanner's version is a minimum, so a later release may be needed. Reissuing certificates and keys needs a change window, and clients that pin the old certificate may need updating.

Band 4 Turn off weak encryption settings on the HTTPS services

Actions 7, 8

The scanner reported older encryption methods on the HTTPS services of the affected hosts. These weaken the protection of encrypted traffic. The scanner did not name the software behind these services, so the location of the settings will vary by host.

Steps for the technician

1. Identify the software behind the HTTPS service on each affected host, and find its TLS settings.
2. Disable the 3DES cipher suites on dc01.corp.example.test, ws14.corp.example.test and app02.corp.example.test at TCP port 443.
3. Disable the RC4 cipher suites on app02.corp.example.test at TCP port 443.
4. Restart the HTTPS service on each host so the change takes effect.
5. Verify by rescanning the 3DES and RC4 plugins on the affected hosts at TCP port 443 and confirming they no longer report.

Restarting the HTTPS services interrupts connections. Some older clients may stop connecting once weak ciphers are removed, so test with the main client applications first.

Band 5 Replace the self-signed certificates and remove medium-strength ciphers

Actions 9, 10

The scanner reported a self-signed certificate on HTTPS services, and medium-strength cipher suites on app02.corp.example.test. These have no CVE, and the scanner rated them lower than the items above. They still matter, because clients cannot confirm the server's identity from a self-signed certificate, and medium-strength ciphers weaken the protection of traffic.

Steps for the technician

1. Confirm the certificate authority to use and the subject names, since the scan does not state them.
2. Request and install certificates from a recognized certificate authority on dc01.corp.example.test and app02.corp.example.test at TCP port 443.
3. On app02.corp.example.test, change the TLS settings on TCP ports 443 and 8443 to remove medium-strength cipher suites, where the application allows it.
4. Check that clients still connect after the change.
5. Restart the services so the changes take effect.
6. Verify by rescanning the self-signed certificate and medium-strength cipher plugins on the affected hosts at the HTTPS ports.

Replacing a certificate can break clients that trust the old one, and removing ciphers may stop older clients from connecting. Plan both with the service owners. The scanner says the cipher change is only possible if the application allows it, and the software behind each port is not named.

Lower-priority items to review

These items sit in the lowest band. The scanner gave no usable fix for them, so a technician needs to decide what applies.

- Review the findings on the affected hosts that have no solution text. Check each one, decide what change applies, and rescan the related plugins after any change.
- Identify the deprecated service component on ws14.corp.example.test, which the scanner reports as end-of-life. The scan does not name it or give an end-of-life date. Ask its vendor for migration guidance, then rescan after it is removed or replaced.

How the findings were prioritised

Findings are sorted into bands, with Band 1 the highest priority. Band 1 holds findings that match CISA's KEV catalog and have recorded ransomware use. Band 2 holds other KEV matches. Band 3 holds findings with a CVE, no KEV match and an urgent score from the scanner; this export has 0 of these. Band 4 holds other CVE findings of meaningful severity. Band 5 holds findings with no CVE but meaningful severity. Band 6 holds low or informational findings.

KEV is CISA's catalog of vulnerabilities it records as known to have been exploited. A finding outside the catalog may still be exploited. The catalog is one input, not a full measure of risk. EPSS scores are not part of this export, so this plan does not use them.

Actions are grouped the way one technician would work in one visit. The bands are never reordered.

What this scan cannot show

This scan is a point-in-time view taken on 2026-08-28 from one vantage point. It cannot show what changed afterwards, what the scanner could not reach, or which other weaknesses exist. It does not show that any system is secure.

Gaps in this export

- The export does not state whether the scanner used logged-in access. The number of hosts scanned with credentials is unknown (unknown), and credential coverage is unknown (unknown).
- The number of validated occurrences with a stated detection quality value is unknown (unknown), so confidence in individual findings cannot be ranked from this export.
- Some occurrences have no CVE (10), no CVSS score (6), or no solution text (5). The scanner could not assess these fully.
- Operating system fingerprint confidence is unknown (unknown).
- The export does not show installed versions for several items, so fix versions are marked as unknown where the data does not give them.

No finding in this report has been confirmed as absent. Rescanning after the work is the check that the change had the intended effect.

Appendix: remediation actions

#	Band	Action	Fix target	Systems	Findings	KEV
1	Band 1	Apply the MS17-010 security update. on 2 systems -> eliminates 3 vulnerable instances across 2 findings.	No version stated; apply the referenced advisory (MS17-010)	2	2	2
2	Band 1	Apply the July 2021 out-of-band security update. on 2 systems -> eliminates 2 vulnerable instances across 1 finding.	unknown	2	1	1
3	Band 1	Apply the August 2020 security update and enforce secure RPC. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	1
4	Band 1	Apply the May 2019 security update. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	1
5	Band 1	Upgrade Log4j to 2.17.1 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	2.17.1	1	1	1
6	Band 2	Upgrade to OpenSSL 1.0.1g or later and reissue certificates. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	1.0.1g	1	1	1
7	Band 4	Reconfigure the service to disable 3DES cipher suites. on 3 systems -> eliminates 3 vulnerable instances across 2 findings.	unknown	3	2	0
8	Band 4	Reconfigure the service to disable RC4. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0
9	Band 5	Install a certificate signed by a recognized authority. on 2 systems -> eliminates 2 vulnerable instances across 1 finding.	unknown	2	1	0
10	Band 5	Reconfigure the affected application, if possible, to avoid the use of medium strength ciphers. on 1 system -> eliminates 2 vulnerable instances across 1 finding.	unknown	1	1	0
11	Band 6	Manually review 2 findings on 3 systems — the scan supplied no solution text; 5 vulnerable instances remain open.	unknown	3	2	0
12	Band 6	Contact the vendor for guidance on migrating away from this component. on 1 system -> eliminates 1 vulnerable instance across 1 finding.	unknown	1	1	0

Technical detail by action

1. Apply the MS17-010 security update. on 2 systems -> eliminates 3 vulnerable instances across 2 findings.

Band 1

Findings	MS17-010: Security Update for Microsoft Windows SMB Server; Microsoft Windows SMBv1 Multiple Remote Code Execution Vulnerabilities
CVEs	CVE-2017-0144, CVE-2017-0143, CVE-2017-0146
Systems	dc01.corp.example.test, ws14.corp.example.test
Services	TCP port 445 (cifs)
Fix target	No version stated; apply the referenced advisory (MS17-010)
Advisories	MS17-010
Scanner plugins	34477, 200101

2. Apply the July 2021 out-of-band security update. on 2 systems -> eliminates 2 vulnerable instances across 1 finding.

Band 1

Findings	Windows Print Spooler RCE (PrintNightmare)
CVEs	CVE-2021-34527
Systems	dc01.corp.example.test, ws14.corp.example.test
Services	TCP port 445 (cifs)
Scanner plugins	151478

3. Apply the August 2020 security update and enforce secure RPC. on 1 system -> eliminates 1 vulnerable instance across 1 finding.

Band 1

Findings	Netlogon Elevation of Privilege (ZeroLogon)
CVEs	CVE-2020-1472
Systems	dc01.corp.example.test
Services	TCP port 445 (cifs)
Scanner plugins	140770

4. Apply the May 2019 security update. on 1 system -> eliminates 1 vulnerable instance across 1 finding.

Band 1

Findings	Microsoft Windows Remote Desktop Services RCE (BlueKeep)
CVEs	CVE-2019-0708
Systems	dc01.corp.example.test
Services	TCP port 3389 (msrdp)
Weakness	CWE-416: Use After Free
Scanner plugins	125313

5. Upgrade Log4j to 2.17.1 or later. on 1 system -> eliminates 1 vulnerable instance across 1 finding.

Band 1

Findings	Apache Log4j 2.x < 2.15.0 Remote Code Execution
CVEs	CVE-2021-44228
Systems	app02.corp.example.test
Services	TCP port 8080 (http)
Fix target	2.17.1
Weakness	CWE-20: Improper Input Validation; CWE-400: Uncontrolled Resource Consumption; CWE-502: Deserialization of Untrusted Data; CWE-917: Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')
Scanner plugins	155999

6. Upgrade to OpenSSL 1.0.1g or later and reissue certificates. on 1 system -> eliminates 1 vulnerable instance across 1 finding. Band 2

Findings	OpenSSL Heartbeat Information Disclosure (Heartbleed)
CVEs	CVE-2014-0160
Systems	app02.corp.example.test
Services	TCP port 443 (https)
Fix target	1.0.1g
Weakness	CWE-125: Out-of-bounds Read
Scanner plugins	73412

7. Reconfigure the service to disable 3DES cipher suites. on 3 systems -> eliminates 3 vulnerable instances across 2 findings. Band 4

Findings	SSL/TLS Birthday attack on 64-bit block ciphers (SWEET32); SSL/TLS 3DES Cipher Suite Vulnerability (Alternate Detection Method)
CVEs	CVE-2016-2183
Systems	app02.corp.example.test, ws14.corp.example.test, dc01.corp.example.test
Services	TCP port 443 (https)
Weakness	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
Scanner plugins	94437, 200102

8. Reconfigure the service to disable RC4. on 1 system -> eliminates 1 vulnerable instance across 1 finding. Band 4

Findings	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
CVEs	CVE-2015-2808
Systems	app02.corp.example.test
Services	TCP port 443 (https)
Weakness	CWE-327: Use of a Broken or Risky Cryptographic Algorithm
Scanner plugins	65821

9. Install a certificate signed by a recognized authority. on 2 systems -> eliminates 2 vulnerable instances across 1 finding. Band 5

Findings	SSL Self-Signed Certificate
Systems	dc01.corp.example.test, app02.corp.example.test
Services	TCP port 443 (https)
Scanner plugins	57582

10. Reconfigure the affected application, if possible, to avoid the use of medium strength ciphers. on 1 system -> eliminates 2 vulnerable instances across 1 finding. Band 5

Findings	SSL Medium Strength Cipher Suites Supported
Systems	app02.corp.example.test
Services	TCP port 443 (https), TCP port 8443 (https)
Scanner plugins	42873

Data sources & licensing

This report uses public data from the sources below. It was extracted and normalized for this report; no source endorses this report. The attribution each source's licence or terms ask for is printed with the source it belongs to.

KEV catalog (Required feed)

Data used: retrieved 2026-10-18.

The KEV database is distributed under the Creative Commons 0 1.0 License (<https://creativecommons.org/publicdomain/zero/1.0/>). Use of the information does not authorize use of the CISA Logo or DHS Seal, nor should such use be interpreted as an endorsement by CISA or DHS.

Source: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json

EPSS (Required feed)

EPSS scores: Exploit Prediction Scoring System (EPSS), FIRST, <https://www.first.org/epss/>, score date 2026-10-18.

JVN iPedia (Vulnerability context)

Data used: last refreshed 2026-10-18 12:28 UTC.

JVN iPedia (<https://jvndb.jvn.jp/en/>), the vulnerability countermeasure information database of the Information-technology Promotion Agency, Japan (IPA), which carries the Japan Vulnerability Notes that JPCERT/CC and IPA publish; read from IPA's public MyJVN data feeds (the English detail feeds and the new/updated feed). Used under the MyJVN API Terms of Use (<https://jvndb.jvn.jp/apis/termsfuse.html>), which IPA applies to its data feeds and under which commercial use, quotation, reproduction and redistribution are not restricted. Records are extracted and normalized for this report; JVN iPedia's affected-version and solution text is quoted as it states it. IPA does not guarantee the information and does not endorse this report.

Source: <https://jvndb.jvn.jp/en/feed/>

MITRE CAPEC (Vulnerability context)

Data used: last refreshed 2026-10-18 12:27 UTC.

CAPEC content: Copyright © 2007–2026, The MITRE Corporation. The MITRE Corporation (MITRE) hereby grants you a non-exclusive, royalty-free license to use Common Attack Pattern Enumeration and Classification (CAPEC™) for research, development, and commercial purposes. Any copy you make for such purposes is authorized provided that you reproduce MITRE's copyright designation and this license in any such copy. CAPEC and the CAPEC logo are trademarks of The MITRE Corporation. Terms of Use: <https://capec.mitre.org/about/termsfuse.html>

Copyright © 2007–2026, The MITRE Corporation. The MITRE Corporation (MITRE) hereby grants you a non-exclusive, royalty-free license to use Common Attack Pattern Enumeration and Classification (CAPEC™) for research, development, and commercial purposes. Any copy you make for such purposes is authorized provided that you reproduce MITRE's copyright designation and this license in any such copy.

MITRE CWE (Vulnerability context)

Data used: last refreshed 2026-10-18 12:27 UTC.

CWE content: Copyright © 2006–2026, The MITRE Corporation. CWE™ is free to use by any organization or individual for any research, development, and/or commercial purposes, per the CWE Terms of Use (<https://cwe.mitre.org/about/termsfuse.html>). The MITRE Corporation hereby grants you a non-exclusive, royalty-free license to use CWE for research, development, and commercial purposes. Any copy you make for such purposes is authorized on the condition that you reproduce MITRE's copyright designation and this license in any such copy. CWE is a trademark of The MITRE Corporation.

Copyright © 2006–2026, The MITRE Corporation. CWE™ is free to use by any organization or individual for any research, development, and/or commercial purposes, per these CWE Terms of Use. Accordingly, The MITRE Corporation hereby grants you a non-exclusive, royalty-free license to use CWE for research, development, and commercial purposes. Any copy you make for such purposes is authorized on the condition that you reproduce MITRE's copyright designation and this license in any such copy.

NVD (Vulnerability context)

Data used: last refreshed 2026-10-18 12:29 UTC.

This product uses the NVD API but is not endorsed or certified by the NVD.

Source: <https://nvd.nist.gov/developers/vulnerabilities>

OWASP Top 10 (Vulnerability context)

Data used: last refreshed 2026-10-18 12:27 UTC.

OWASP Top 10:2025, © 2021–2025 OWASP Top 10 Team (<https://owasp.org/Top10/2025/>), licensed under the Creative Commons Attribution-ShareAlike 4.0 International License (<https://creativecommons.org/licenses/by-sa/4.0/>). Category identifiers and titles are reproduced unmodified. A category shown beside a finding is a public cross-reference, not an OWASP assessment or a statement of compliance; OWASP does not endorse this report.

Values this report attributes to NVD (CVSS scores, versions and vectors, CWE identifiers and reference addresses) are reproduced as NVD states them; reference tags are restated in words, and CWE names are MITRE's (CWE), not NVD's.

The words in this report were written by an AI model (claude-haiku-5-5) and checked automatically before release. Every count, priority band and KEV status comes from the scoring engine, not the model. Validate changes before applying them. Rules 7ee05e85a8d6.