

RiskSnap Evidence Pack



Software Supply Chain Risk Evidence for CMMC Level 2

Synthetic example — fictional client and commentary

Prepared by Meridian Assurance Partners · assurance@meridian.example

Generated: 2026-10-04T06:43:29+00:00

Scan Metadata

Tool	RiskSnap v0.8.0
Scan started (UTC)	2026-10-04T06:43:21+00:00
Scan completed (UTC)	2026-10-04T06:43:22+00:00
Input file	northwind_current.cdx.json (3,930 bytes)
Input SHA-256	35f0ae8147b1bbef...
OSV data fetched (UTC)	2026-10-04T06:43:21+00:00
OSV source status	Reached — data applied
CISA KEV fetched (UTC)	2026-10-04T06:43:21+00:00
CISA KEV source status	Reached — data applied
NVD enrichment	not used

Executive Summary

Total scanned components: 9

Rows in this export: 9

Risky components (in this view): 5

Known exploited (CISA KEV): 0

URGENT: 0 HIGH: 1 MED: 1 LOW: 3 Clean: 3 SKIPPED: 1

Medium/Low findings are summarized below; full evidence is in Appendix A.

Scan Coverage

1 unpinned component(s) were not scanned for vulnerabilities. Pin to exact versions (e.g., pkg==1.2.3) to enable scanning.

Top Priority Findings (URGENT/HIGH) - Top 10

Bucket	Component	Version	Ecosystem	Exploited	Severity	CVEs	Fix
HIGH	commons-text	1.9.0	Maven	No	9.5	CVE-2022-42889	

Findings Summary

Medium Findings (n=1)

- postgresql 42.7.2 - CVE-2026-42198 - CVE-2026-42198 (CVSS 8.0). pgjdbc: Unbounded PBKDF2 iterations in SCRAM authentication allows CPU exhaustion DoS. Plan patching in normal cycle.

Low Findings (n=3)

- commons-lang3 3.14.0 - CVE-2025-48924 - Low risk or insufficient severity data. Monitor and review.
- log4j-api 2.17.2 - CVE-2026-49844 - Low risk or insufficient severity data. Monitor and review.
- log4j-core 2.17.2 - CVE-2025-68161, CVE-2026-34477, CVE-2026-34480 - Low risk or insufficient severity data. Monitor and review.

Clean Components (n=3)

- guava 33.0.0-jre - No CVE IDs - No known vulnerabilities found in current databases. Continue monitoring.
- jackson-annotations 2.16.1 - No CVE IDs - No known vulnerabilities found in current databases. Continue monitoring.
- slf4j-api 2.0.12 - No CVE IDs - No known vulnerabilities found in current databases. Continue monitoring.

Skipped Components (n=1)

- telemetry-agent - No CVE IDs - Unpinned dependency — not scanned for vulnerabilities. Pin to an exact version (e.g., pkg==1.2.3) to enable scanning.

Appendix A: Full Findings Table

Severity Bucket	Component	Version	Ecosystem	CVE IDs	Exploited (KEV)	Fix Available	Fix Version	Max Severity	Why It Matters
HIGH	commons-text	1.9.0	Maven	CVE-2022-42889	No	No		9.5	CVE-2022-42889 (CVSS 9.5). Arbitrary code execution in Apache Commons Text. Prioritize patching soon.
MED	postgresql	42.7.2	Maven	CVE-2026-42198	No	No		8.0	CVE-2026-42198 (CVSS 8.0). pgjdbc: Unbounded PBKDF2 iterations in SCRAM authentication allows CPU exhaustion DoS. Plan patching in normal cycle.

Severity Bucket	Component	Version	Ecosystem	CVE IDs	Exploited (KEV)	Fix Available	Fix Version	Max Severity	Why It Matters
LOW	commons-lang3	3.14.0	Maven	CVE-2025-48924	No	No			Low risk or insufficient severity data. Monitor and review.
LOW	log4j-api	2.17.2	Maven	CVE-2026-49844	No	No			Low risk or insufficient severity data. Monitor and review.
LOW	log4j-core	2.17.2	Maven	CVE-2025-68161, CVE-2026-34477, CVE-2026-34480	No	No			Low risk or insufficient severity data. Monitor and review.
CLEAN	guava	33.0.0-jre	Maven	-	No	No			No known vulnerabilities found in current databases. Continue monitoring.
CLEAN	jackson-annotations	2.16.1	Maven	-	No	No			No known vulnerabilities found in current databases. Continue monitoring.
CLEAN	slf4j-api	2.0.12	Maven	-	No	No			No known vulnerabilities found in current databases. Continue monitoring.
SKIPPED	telemetry-agent		Maven	-	No	No			Unpinned dependency — not scanned for vulnerabilities. Pin to an exact version (e.g., pkg==1.2.3) to enable scanning.

Remediation Checklist

- Patch URGENT items immediately (known exploited vulnerabilities).
- Apply available fixes for HIGH items next (CVSS >= 9.0).
- Pin unpinned dependencies where possible to improve stability.
- Validate upgrades in CI/CD and redeploy with updated lockfiles.
- Re-run RiskSnap after remediation to confirm risk reduction.

Disclaimer

This evidence pack documents software dependency vulnerability analysis suitable for supporting CMMC Level 2 controls related to vulnerability scanning (RA.L2-3.11.2), vulnerability remediation (RA.L2-3.11.3), system flaw identification (SI.L2-3.14.1), and software component inventory (CM.L2-3.4.1). This documentation contributes to the body of evidence required for these controls but does not by itself satisfy any single control. Final determination of compliance is the responsibility of the assessing organization.

RiskSnap is an automated analysis tool. Results are based on public vulnerability databases (OSV, CISA KEV) which may not be complete or current. This report does not guarantee full compliance, does not cover all vulnerability types, and is not a substitute for professional security review or formal CMMC assessment. Users are responsible for final validation. Generated by Meridian Assurance Partners.

No uploads stored. Generated in-session.