

RiskSnap Remediation Progress Report



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

Comparison Metadata

Project	Northwind Avionics
Previous scan	3d678b76 2026-10-04T06:43:19+00:00
Current scan	6b05228f 2026-10-04T06:43:22+00:00
Time span	0 days
Tool version	0.8.0

Executive Summary

Severity	Components (Before → After)	Findings Closed	Findings Added	Findings Outstanding
URGENT ✓	1 → 0	4	0	0
HIGH	1 → 1	0	0	1
MED	1 → 1	0	0	1
LOW	2 → 3	0	0	5
CLEAN	3 → 3	0	0	0
SKIPPED	0 → 1	0	0	0
TOTAL (risky)	5 → 5	4	0	7

Notes

Input file changed: 'northwind_baseline.cdx.json' → 'northwind_current.cdx.json'. Delta reflects both file and database changes.

Closed Findings (Remediation Progress)

Component	CVE	Version	Bucket	Severity
log4j-core	CVE-2021-44228	2.14.0 → 2.17.2	URGENT	9.5
log4j-core	CVE-2021-44832	2.14.0 → 2.17.2	URGENT	9.5
log4j-core	CVE-2021-45046	2.14.0 → 2.17.2	URGENT	9.5

Component	CVE	Version	Bucket	Severity
log4j-core	CVE-2021-45105	2.14.0 → 2.17.2	URGENT	9.5

New Findings (Action Items)

No new findings in this period.

Outstanding Findings (POA&M; Items)

Component	CVE	Version	Bucket	Severity
commons-text	CVE-2022-42889	1.9.0	HIGH	9.5
postgresql	CVE-2026-42198	42.7.2	MED	8.0
commons-lang3	CVE-2025-48924	3.14.0	LOW	—
log4j-api	CVE-2026-49844	2.17.2	LOW	—
log4j-core	CVE-2025-68161	2.17.2	LOW	—
log4j-core	CVE-2026-34477	2.17.2	LOW	—
log4j-core	CVE-2026-34480	2.17.2	LOW	—

Component Inventory Changes

Added Components

- telemetry-agent (Maven) — v?

Version-Changed Components

- log4j-api (Maven) — 2.14.0 → 2.17.2
- log4j-core (Maven) — 2.14.0 → 2.17.2

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). 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.