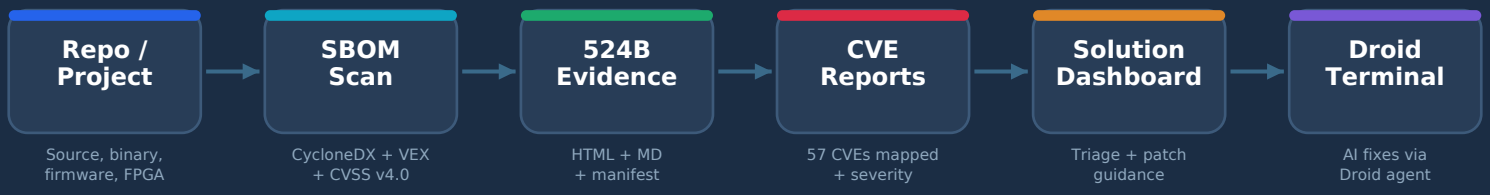
FDA EDITION • MEDICAL DEVICE CYBERSECURITY

Submission-Ready Evidence for Section 524B

The Most FDA-Ready SBOM • HBOM • DataBOM Analysis Tool

From SBOM to VEX to continuous monitoring - the engineering evidence behind FDA premarket cybersecurity submissions.

SBOMATOR® WORKFLOW



Section 524B | **CVSS v4.0** | **HBOM + FPGA** | **Droid-as-Judge**

Evidence preparation for cyber-device engineering teams

What the FDA expects from cyber devices

Section 524B requires manufacturers to connect secure-development plans, vulnerability operations and machine-readable product inventory.

STATUS MAPPED

(b)(1)(A) • SBOM

Generate and maintain product software inventory

STATUS MAPPED

(b)(1)(B) • Monitor

Monitor, identify and address vulnerabilities

STATUS MAPPED

(b)(1)(C) • Patch

Design, develop and maintain patch/update processes

STATUS MAPPED

(b)(1)(D) • Communicate

Coordinated vulnerability disclosure and communication

STATUS MAPPED

(b)(3) • Machine-readable

CycloneDX/SPDX SBOM with NTIA minimum elements

STATUS MAPPING

COMPLIANT • PARTIAL • NON-COMPLIANT • NEEDS INPUT

GUIDANCE ALIGNMENT

Aligned to the February 2026 final guidance context and its relationship with QMSR / ISO 13485 quality-system controls. Manufacturer interpretation and validation remain required.

From shipped build to reviewable evidence

A traceable workflow turns build inventory into vulnerability decisions and a Section 524B evidence package.

NTIA minimum elements

Supplier, name, version, PURL, dependencies, author and timestamp in machine-readable CycloneDX.

Lifecycle support

Support status and end-of-support dates remain visible beside component evidence.

VEX for every CVE

Affected, not affected or under investigation, with justification and response context.

524B status report

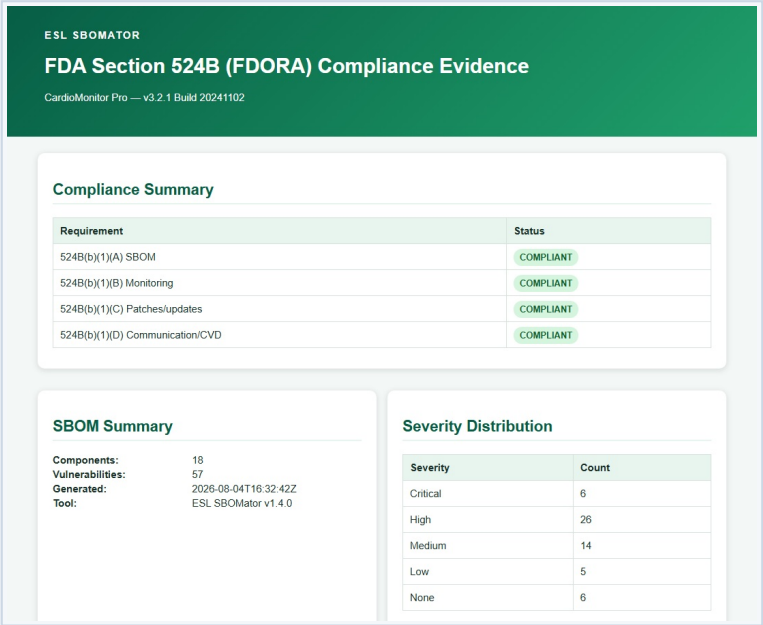
COMPLIANT / PARTIAL / NON-COMPLIANT / NEEDS INPUT mapping for review.

Submission-ready means organized, reviewable evidence — not guaranteed compliance or approval. Manufacturer review, validation, risk acceptance and formal approval remain required.

Generated evidence in review

Every SBOMator™ scan produces a self-contained, printable Section 524B evidence package — no manual formatting required.

COMPLIANCE SUMMARY + SEVERITY DISTRIBUTION



ESL SBOMATOR

FDA Section 524B (FDORA) Compliance Evidence

CardioMonitor Pro — v3.2.1 Build 20241102

Compliance Summary

Requirement	Status
524B(b)(1)(A) SBOM	COMPLIANT
524B(b)(1)(B) Monitoring	COMPLIANT
524B(b)(1)(C) Patches/updates	COMPLIANT
524B(b)(1)(D) Communication/CVD	COMPLIANT

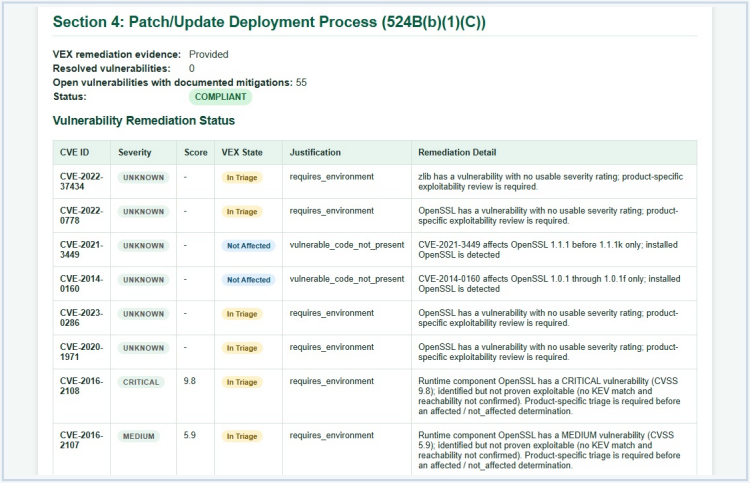
SBOM Summary

Components: 18
Vulnerabilities: 57
Generated: 2026-08-04T16:32:42Z
Tool: ESL SBOMator v1.4.0

Severity Distribution

Severity	Count
Critical	6
High	26
Medium	14
Low	5
None	6

SECTION 4: VULNERABILITY REMEDIATION STATUS TABLE



Section 4: Patch/Update Deployment Process (524B(b)(1)(C))

VEX remediation evidence: Provided
Resolved vulnerabilities: 0
Open vulnerabilities with documented mitigations: 55
Status: COMPLIANT

Vulnerability Remediation Status

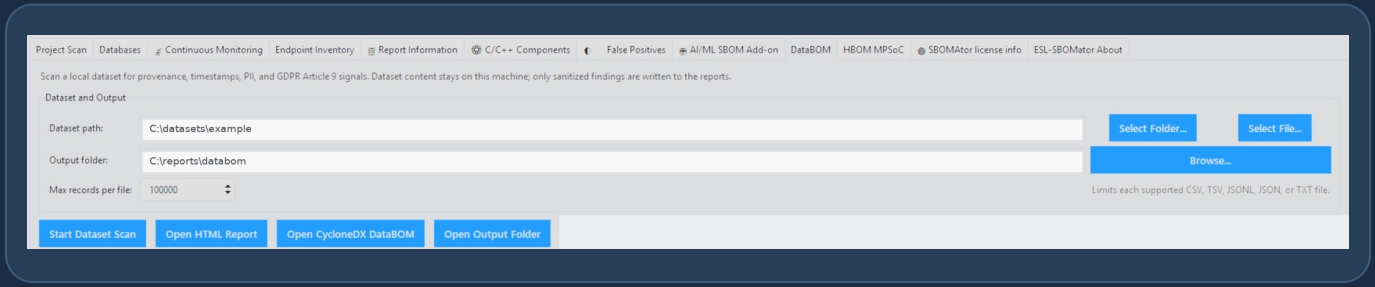
CVE ID	Severity	Score	VEX State	Justification	Remediation Detail
CVE-2022-37434	UNKNOWN	-	In Triage	requires_environment	zlib has a vulnerability with no usable severity rating; product-specific exploitability review is required.
CVE-2022-0778	UNKNOWN	-	In Triage	requires_environment	OpenSSL has a vulnerability with no usable severity rating; product-specific exploitability review is required.
CVE-2021-3449	UNKNOWN	-	Not Affected	vulnerable_code_not_present	CVE-2021-3449 affects OpenSSL 1.1.1 before 1.1.1k only; installed OpenSSL is detected
CVE-2014-0160	UNKNOWN	-	Not Affected	vulnerable_code_not_present	CVE-2014-0160 affects OpenSSL 1.0.1 through 1.0.1f only; installed OpenSSL is detected
CVE-2023-0286	UNKNOWN	-	In Triage	requires_environment	OpenSSL has a vulnerability with no usable severity rating; product-specific exploitability review is required.
CVE-2020-1971	UNKNOWN	-	In Triage	requires_environment	OpenSSL has a vulnerability with no usable severity rating; product-specific exploitability review is required.
CVE-2016-2108	CRITICAL	9.8	In Triage	requires_environment	Runtime component OpenSSL has a CRITICAL vulnerability (CVSS 9.8); identified but not proven exploitable (no KEV match and reachability not confirmed). Product-specific triage is required before an affected / not_affected determination.
CVE-2016-2107	MEDIUM	5.9	In Triage	requires_environment	Runtime component OpenSSL has a MEDIUM vulnerability (CVSS 5.9); identified but not proven exploitable (no KEV match and reachability not confirmed). Product-specific triage is required before an affected / not_affected determination.

WHAT YOU GET

HTML + Markdown + manifest - Color-coded severity and VEX-state badges - CVE ID, CVSS score, justification and remediation detail per row - COMPLIANT / PARTIAL / NON-COMPLIANT / NEEDS INPUT status mapping - Printable and submission-ready.

CycloneDX 1.7 ML-BOM evidence for AI/ML datasets

Inventory local training, validation and test data; expose provenance and privacy-review gaps without uploading sensitive dataset content.



CycloneDX ML-BOM

Strict 1.7 data components, source dependencies and schema validation; 1.6 compatibility is available.

Dataset provenance

Inventory source domains, record counts, collection periods and evidence-completeness scores.

Privacy review signals

Detect and mask potential PII excerpts, flag special-category indicators and identify mandatory human assessments.

SELECT Local file or folder → **PARSE** JSONL, CSV, Parquet + text → **SCREEN** PII + Art. 9 indicators → **REVIEW** Risk + evidence gaps → **EXPORT** HTML + CycloneDX ML-BOM

IMPORTANT REGULATORY BOUNDARY

DataBOM provides dataset inventory and automated risk signals. It does not establish clinical validity, statistical integrity, informed consent, IRB/ethics approval, de-identification, electronic-record compliance, GCP compliance or FDA clearance. Sponsor and manufacturer review remains required.

CVSS v4.0 and multi-source correlation

NVD, OSV and Grype findings are enriched with CISA KEV exploitation status and FIRST EPSS prioritization.

NVD | OSV | GRYPE | KEV | EPSS | CVSS 4.0

Supports CVSS v4.0 vectors and ratings alongside v3.x — parses, scores and maps severity from both standards.

NVD + OSV correlation

Cross-source identity and advisory evidence

KEV exploitation status

Known exploitation changes response urgency

EPSS prioritization

Probability evidence helps order remediation

CVSS v4.0 parsing

Mixed v3/v4 CycloneDX ratings and severity mapping

CONSENSUS-STANDARD CONTEXT

FDA recognized CVSS v4.0 as consensus standard STG #13 in 2026. SBOMator supports its vectors and ratings; it does not claim certification as an official score engine.

Droid as Judge: AI triage in the terminal

A strongly controlled agent workflow converts selected findings into reviewable reachability, remediation and VEX evidence.

ANALYZE CHECKED CVEs IN AGENT →

Load the SBOM report • filter by severity, classification and VEX state • select CVEs • launch Droid in the real embedded terminal.

1 Load + filter

Components, CVEs and evidence

2 Droid judges

False positive? Not affected? Reachable?

3 Resolve

Smallest safe fix or VEX justification

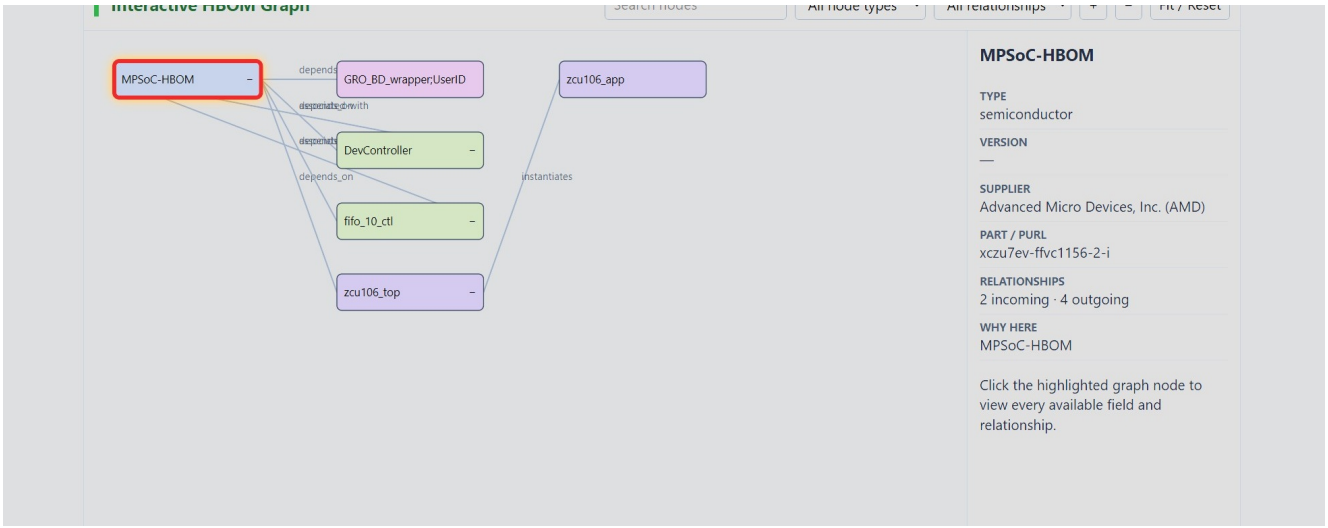
RESTRICTED AUTONOMY — ENGINEER RETAINS CONTROL

Droid runs with --auto medium and --disabled-tools Edit. It can read and create files, but cannot modify existing files. Droid explains reachability and proposes evidence; the manufacturer reviews and validates every decision.

Factory and Droid are marks of Factory AI. Used for integration; no partnership or endorsement is implied.

Product-scoped MPSoC hardware + firmware evidence

Reconcile Vivado, HLS, bitstream, HDL, firmware and linked-software artifacts into validated, traceable HBOM evidence for a controlled device release.



Discover + reconcile

Parse Vivado projects/IP, Vitis HLS, VHDL and .bit headers; preserve evidence and flag target-part conflicts instead of guessing.

Link hardware + software

Link MPSoC, programmable logic, firmware, boot artifacts and per-core SBOMs with searchable runs-on and contains relationships.

Validate + control change

Export CycloneDX 1.6, SPDX 2.3, VEX, CISA, Jenkins and HTML; add quality scoring, baseline drift and SHA-256 integrity evidence.

Optional licensed HBOM module • Optional Ed25519 manifest signing • Board-level PCB procurement BOM remains separate

Evidence doesn't stop at submission

Section 524B(b)(2) requires postmarket updates and patches; retained evidence must follow the product after release.

EDR-SBOM monitoring

Endpoint inventory reflects deployed reality

Integrity drift

Detect changes against the established baseline

New-CVE + malware alerts

Email/webhook routing for new CVEs and OSV-flagged malicious packages

Report diffing

Track remediation and evidence progress

Audit chain

Retain reports, deltas and decision history

POSTMARKET LOOP

Discover → assess → patch → communicate → retain

SBOM is a living document

Maintain it under ISO 13485 configuration management, with manufacturer-controlled review and approval.

Build your FDA evidence with engineering depth

Connect product inventory, vulnerability decisions, hardware provenance and postmarket monitoring in one reviewable evidence model.

What SBOMator™ covers

- CycloneDX SBOM + NTIA elements
- CycloneDX 1.7 ML-BOM + dataset provenance
- Vulnerability correlation + CVSS v4.0
- VEX decisions and 524B status mapping
- MPSoC HBOM + baseline, drift and integrity...

What remains your responsibility

- Product risk management and clinical context
- Evidence review and validation
- Patch and communication decisions
- Risk acceptance and formal approval
- Regulatory interpretation and submission

SBOMator™ supports compliance evidence preparation and maps available evidence to Section 524B expectations. Manufacturer review, validation, risk acceptance and formal approval remain required. This brochure is informational and does not constitute legal advice or guarantee FDA clearance.

Engineering Software Lab

www.eswlab.com • sales@eswlab.com