

Software Bill of Materials (SBOM)

SBOM

239 total components in package
Verified Components: 157

Firmware Health Score F

Issues Detected

Attestation Signature Mismatch	12
Verification Hash Missing	7
Incorrect Firmware Signature	5
Risk Level Detected	6
High Risk	4
Medium Risk	2
Unknown Digital Signatures	4
Outstanding Mitigations	1
Potential Data Compromise	1

Major security risks detected. Unsafe to install or run. Remove and restore to last known safe version.

What is SBOM?

A software bill of materials (SBOM) declares the inventory of components used to build a software artifact such as a software application. According to CISA, SBOM “..is a nested inventory , a list of ingredients that make up software components.”

It is a key building block in software security and software supply chain risk management. An SBOM report details the firmware components, libraries, tools, utilities, and build environment of an image (binary). AMI’s SBOM utilities support AMI Aptio and MegaRAC projects. Once licensed, developers can generate spec-compliant SBOM reports for their projects.

AMI SBOM Offering Overview

Product	SBOM Format	Version
Aptio V	CycloneDX	1.5
	SPDX	2.3
MegaRAC SP-X	CycloneDX	1.5
	SPDX	2.3
MegaRAC OneTree	SPDX	2.3

Figure 1: AMI Meridian SBOM User Interface

The screenshot shows a web-based interface for managing software vulnerabilities. At the top, there's a navigation bar with links for 'Vulnerability Management System', 'Project Name' (set to '1.2.1.TAIIPEI_R2C2_00.00.400322.01.074'), and 'Project Status' (set to 'Completed'). Below the navigation is a main dashboard area. On the left, there are three cards: 'Total Vulnerabilities' (36), 'Fixed' (17), and 'Not Fixed' (19). In the center, there's a pie chart titled 'Vulnerability By Party' showing the distribution between '1st Party' (blue), '2nd Party' (green), and '3rd Party' (yellow). To the right, there's another pie chart titled 'Vulnerability By Severity' showing the distribution between 'Info' (red), 'Low' (orange), 'Medium' (yellow), and 'Critical' (green). At the bottom, there's a section titled 'Vulnerability Addressed History' with a table showing a list of security advisories and their status.



Key Features

- Full/Complete Report Generation
 - ✓ Open-source components
 - ✓ AMI IP
 - ✓ Silicon Vendor IP
- Partial Report Generation (Non-NDA)
 - ✓ Open-source components
 - ✓ Third-Party IP
 - ✓ Can be shared Publicly
 - ✓ Can be embedded into FW binary
- Module-level Report Generation
- Security Patch Tracking
- Security Advisory and CVE Mapping
- Active Module Filtering
- IDE (VeB) and CLI Support
- Intuitive Web-UI and API Support
- Regulatory Compliance (NIST, CISA, etc.)
- Legacy Project SBOM Support Enablement
- SBOM integration into Final Firmware Image (ACPI)
- Integration with AMI Vulnerability Management Service (VMS)

SPDX-CycloneDX Mapping

This table maps baseline attributes across SPDX and CycloneDX. In addition to the baseline attributes, Authors should conform to the specifications of their chosen SBOM format.

Table 1: Mapping baseline component information to existing formats

Attribute	ISO/IEC 5962:2021 (SPDX v2.3)ISO/IEC 5962:2021	ISO/IEC 5962:2021 (SPDX v3.0)	CycloneDX v1.2-1.6
Author Name	(6.8) Creator:	Core. CreationInfo.createdBy	bom.metadata.authors
Timestamp	(6.9) Created:	Core. CreationInfo.created	bom.metadata.timestamp
Type	(6.10) CreatorComment:	Software. Sbom.sbmotype	bom.metadata.properties[]
Primary Component	(11.1) Relationship: DESCRIBES CONTAINS	Software. Sbom.rootElement	bom.metadata.component[]
Component Name	(7.1) PackageName:	Software. Package.name	bom.components[].name
Version String	(7.3) PackageVersion:	Software. Package.	bom.components[].version
Supplier Name	(7.5) PackageSupplier:	Software. Package.	bom.metadata.supplier bom.components[].supplier
Cryptographic Hash	(7.10) PackageChecksum: (7.9) PackageVerificationCode:	Software. Package.	bom.components[].hashes[]
Unique Identifier	(6.5)SPDX Document Namespace (7.2) SPDXID:	(6.5)SPDX Document Namespace (7.2) SPDXID:	bom.components[].cpe bom.components[].purl bom.components[].swid bom.components[].omnibuild bom.components[].swhid
Relationships	(11.1) Relationship: DESCRIBES CONTAINS	(11.1) Relationship: DESCRIBES CONTAINS	bom.dependencies[]
License	(7.15) PackageLicenseDeclared: (7.13) PackageLicenseConcluded: (7.14) LicenseInfoFromFiles:	(7.15) PackageLicenseDeclared: (7.13) PackageLicenseConcluded: (7.14) LicenseInfoFromFiles:	bom.components[].licenses[]
Copyright Holder	(7.17) PackageCopyrightText:	(7.17) PackageCopyrightText:	bom.components[].copyright

CISA document: <https://www.cisa.gov/resources-tools/resources/framing-software-component-transparency-2024>