NETRISE

A GUIDE TO

Software Bill of Materials

Software component security is essential to safeguarding XIoT devices and the networks they operate on.

Overview

Performing comprehensive vulnerability and threat analyses of your devices requires accurate and complete software bills of materials (SBOMs).

A software bill of materials is a list of every software component running on an Extended Internet of Things (XIoT) device. XIoT comprises the Internet of Things (IoT), Operational Technology (OT), medical devices, and other connected devices. SBOMs empower both device manufacturers and asset owners by providing transparency into what's running in a device at the component level, allowing security teams to quickly assess and mitigate threats at the most granular level.

What Are SBOMs and Why Are They Important?

Think of a software bill of materials as an official ingredient list for a piece of software within a device. These parts, such as libraries and modules, can be open-source or owned, free or paid, and the information can be easily accessible or limited.

Industry experts refer to XIoT devices as black boxes because there is little visibility into what is running inside them. Firmware and software components are largely unknown without creating an SBOM, and not knowing what is running within the devices on your network puts your organization at risk for cyber threats, noncompliance, loss of business, and more.

SBOMs vs HBOMs

SBOM

A software bill of materials enables software developers, device manufacturers, and end users of devices to understand and reduce the risks of devices. SBOMs allow security teams to quickly identify any vulnerabilities should they arise.

Learn About Compliance Adherence

HBOM

A hardware bill of materials (HBOM) lists every physical piece used to build a device. An HBOM provides manufacturers and asset owners with the information necessary to make decisions based on the origins and makeup of a given product.

Learn About Inventory & Querying

SBOM Benefits

- Recognize and prevent established vulnerabilities.
- Lower operating expenses due to increased efficiencies and decreased unforeseen, unscheduled tasks.
- Recognize and address security obligations.
- Facilitate the assessment of the inherent risks in XIoT firmware and software.
- Take measures to reduce risks (such as updating and implementing alternative safeguards for new vulnerabilities).
- Determine and oversee licensing requirements.

Just to be clear, we want to emphasize that merely having an SBOM doesn't make your networks any more secure on its own. If the security of the components within an SBOM are not directly improved, attackers are just as likely to attack. What actually reduces risks and improves cybersecurity are the actions you take with the insights SBOMs provide.

Why SBOMs Are Important

For Device Manufacturers

- Allows for rapid response to risks and vulnerabilities associated with software components
- Enables compliance with supply chain security standards and regulations
- Provides downstream customers with necessary supply chain information

Device Manufacturers SBOM Management Brief

For Asset Owners

- Enables rapid response to risks and vulnerabilities associated with software components
- Improves the visibility and security of firmware, software, devices, and networks
- Allows security teams to catch software supply chain exposures before adding or patching devices

Device Owners SBOM Management Brief

Executive Order 14028

In May 2021, the Biden Administration announced Executive Order 14028 in an effort to improve the nation's cybersecurity. The mandate requires device manufacturers to pay attention to and illuminate their upstream and downstream supply chains. To do this, they must generate and maintain an SBOM for each device.

The coordination of enforcing Executive Order 14028 is still in its beginning phases, but we expect enforcement will be in the form of government audits, with noncompliance resulting in fines. This executive order represents a first step toward broader government regulation requiring effective SBOM management from manufacturers and indicates the potential for loss of revenue and business growth opportunities for those who are slow to adapt.

How SBOMs Are Created

SBOM creation via the NetRise platform starts with inspecting the current build of the product or firmware with Binary Composition Analysis (BCA). This deep, proprietary analysis provides visibility into all the components used to create software or firmware. The automated reverse engineering capabilities of the NetRise platform can provide organizations with as much as a 99.98% reduction in time expenditure, per DoD, GSA, and NASA estimates. The machine learning-powered scalability, comprehensiveness, and efficiency of the NetRise platform are unmatched in the current SBOM management market.

Think of SBOM generation like a ZIP file. To open it, you have to unzip and decrypt it. There may be one file or it may have many files. The same is true of an XIoT device. The NetRise platform unpacks it, decompresses it, and decrypts it to understand the components.

What Should Be Included in an SBOM?

An SBOM should contain the following information:

- Author
- Supplier
- Component name
- Version string
- Component hash
- Unique identifier and relationship
- Licensing
- Pedigree
- Provenance (if available)

How Often Do I Need to Update an SBOM?

An SBOM should be updated whenever there are changes to the components that make up software within a device. If new software/ firmware is released or a patch is made, an SBOM should be generated.

Leveraging SBOMs for ICS Security

NetRise CEO Thomas Pace gives an in-depth webinar on how ICS security professionals can utilize SBOM management to reduce risk and improve cybersecurity.

Watch the Webinar

How SBOMs Help During Cyber Attacks

Most often, an attacker compromises the supply chain where the firmware is created, which is why firmware security is so important. Once the firmware is compromised, the device can be leveraged in a number of ways. Signs of breach may include noticing the device exhibiting abnormal behavior or being unable to login to or control the device. Oftentimes, the compromised device represents an open door into the rest of your organization.

Security teams can leverage SBOMs to find vulnerabilities in device firmware and software before, during, or after a cyber incursion. The NetRise Platform continuously scans the National Vulnerability Database (NVD), the CISA Known Exploited Vulnerabilities Catalog (KEV), Threat Actor Groups, BOTNETs, and more to provide insight into the exploitability of risks. NetRise also alerts you to vulnerabilities within your network and prioritizes risks based on the potential for impact, enabling quicker and more effective mitigation efforts.

Identifying vulnerabilities allows:

- Device manufacturers to release patches or other remediation options
- Asset owners to find and undertake mitigations independently of device manufacturers
- Identification of affected software across all devices

The NetRise platform helps security teams understand their risks, prioritizes vulnerabilities, and recommends a path to remediation. With NetRise Trace, users can quickly trace impacted assets with a single query, creating a comprehensive graph of affected software supply chain components and their associated vulnerabilities.

SBOM Misconceptions

Some may wonder if SBOMs provide a supply chain or intellectual property roadmap for hackers. While this is theoretically true, it's important to remember these facts.

- SBOMs serve more as a roadmap for the defender, not the attacker.
- Attackers don't need SBOMs or insider foresight to cause harm.
- Defenders struggle to pinpoint software components, whereas attackers and their tools excel at it.
- Attackers of any single product can already find human-readable targets.
- You have the option to keep or share your exclusive source code.
- Upstream, third-party, and open-source software suppliers own all the intellectual property related to supply chain components.

SBOMs and VEX

The Vulnerability Exploitability Exchange (VEX) provides additional information on whether a product may be affected by a specific vulnerability and, if affected, whether there are actions recommended to remediate it.

VEX is highly flexible and can be used to communicate vulnerability information to users in a number of ways. For example, a VEX may be used to assert the vulnerability status for all known vulnerabilities in a given product or to communicate that a single, high-profile vulnerability isn't applicable to a product. VEX consumers should communicate with their suppliers to understand the specific use case a particular VEX document is meant to achieve.

While they are designed to work together, VEX does not require an SBOM and SBOMs do not require VEX. The increased transparency afforded by SBOMs makes VEX a useful way to communicate with stakeholders at scale.

Compliance
SBOMs serve more as a roadmap for the defender, not the attacker.

Security
Customers need firmware and software component visibility to ensure their network is protected.

Procurement
Asset owners will require SBOMs for assurance that their network will remain secure when devices are installed or updated.

Sales
Prove transparency in the RFP process and save customers the time it takes to request an SBOM.

Compliance
Auditors will demand SBOMs to analyze devices and networks for compliance.

Security
Security teams will use the SBOM to monitor their environment and react to new vulnerabilities.

Protect Your Supply Chain with NetRise

NetRise SBOMs are based on Binary Composition Analysis rather than software composition analysis (SCA). The most common approach to creating an SBOM is by going into the code and looking for what software was used, but that approach only provides a partial answer because it's only one link in the supply chain.

BCA analyzes the final product, which gives a much more detailed and accurate listing of components. The NetRise Platform also allows customers to work with SBOMs from multiple sources (upload/combine/enrich/download), which is particularly important for device manufacturers who may be sourcing software components from a collection of internal, external, and open-source sources.

Benefits of using NetRise for SBOM management:

- Visibility into your software supply chain
- Aggregate data from multiple sources
- Import, enrich, normalize, and export of both SPDX and CycloneDX formats
- SBOM storage library, no matter who created it
- AI-powered semantic search across all assets with NetRise Trace

Ready to See NetRise in Action?

Schedule a NetRise platform demo, and learn more about how NetRise can improve your IoT security posture today.

Contact Us

NETRISE

netrise.io | sales@netrise.io