Fortress

ABSOLUTELY CRITICAL

Software Bill of Materials (SBOM)

Software Supplier Overview

Fortress Information Security, LLC
Phone: 855.FORTRESS
250 S. Orange Ave., Suite 500, Orlando, FL 32801

Fortress SBOM Software Supplier Overview

About Fortress

Fortress Information Security ("Fortress") provides cyber risk management solutions for mission critical supply chains including services for third-party risk management, product security and risk management, file integrity assurance, continuous monitoring, and remediation to support an overall zero trust security model. Fortress specializes in critical infrastructure sectors and supports major utilities, oil and gas, government defense entities, healthcare and more.

Fortress is working on behalf of the utility industry to create and maintain the North American Energy Software Assurance Database (NAESAD). The NAESAD is a repository of software transparency artifacts for applications used within the energy sector. Software Bill of Materials (SBOMs) are key artifacts that demonstrate secure software development practices.

Fortress also operates the Asset to Vendor Network ("A2V Network"), which is a collaborative, information-sharing network of utilities and utility vendors, which is used by NAESAD to provide secure permissioned sharing.

How does Fortress protect your data?

Fortress Information Security holds SOC 2 Type 2 and NIST SP 800-171 certifications. The Fortress Platform secures data in transit by requiring TLS 1.2+ security protocols. Data at rest is stored on encrypted volumes, and files uploaded to the platform are encrypted a second time at the application-level utilizing AES-256 encryption algorithms. Fortress Platform data access is protected via multi-factor authentication.

What information are we requesting?

We are requesting the following information on your products formatted in one of the two major SBOM formats - CycloneDX or SPDX. We can also provide advice and answer questions on SBOM creation and formats as needed.

Vulnerability Exploitability eXchange (VEX) documents, if available, should also be provided. VEXs are machine-readable documents which explain if a product is affected by a discovered vulnerability. VEXs may be in CycloneDX v1.4 or Common Security Advisory Framework (CSAF) v2.0 formats.

The tables below list the minimum data requirements to be included in the SBOM and VEX documents.

Product Information			
Product Name	Product Supplier Name	Product Version	Product Identifier
Product Type	Product Description	Product License	Cryptographic Hash of Product File
Download URL of Product			

Component Information			
Component Name	Component Supplier	Component Version	Component Identifier
Component Type	Component Description	Component Licenses	Cryptographic Hash of the Component
Download URL of Component	Version Control System URL	Component Relationships	

Vulnerability Exploitability eXchange (VEX) Information			
Product Name	Product Supplier Name	Product Version	Product Identifier
Vulnerability Identifier	Vulnerability Description	Exploitability Status	Remediation Information
Document Author	Document Timestamp		

Why should you provide SBOMs?

Open-source libraries and third-party software component dependencies represent a major vector for the propagation of vulnerabilities. Increasingly, asset owners are concerned with what pieces of software are used in products deployed in their systems. Knowledge of what software components are used in a device can aid in remediation strategies in the inevitable event new vulnerabilities are discovered for a particular third-party software library. In addition to cybersecurity concerns, certain customers in the Federal space have restrictions on 'countries of origin' for hardware and software they are allowed to use. This restriction applies to software as well and Fortress will use SBOM information provided to generate provenance information when possible.

This is also an opportunity to share VEX (Vulnerability Exploitability eXchange) information. Often the software components found inside software have vulnerabilities associated with them. Without context, customers are left with a list of vulnerabilities, often in the hundreds. You are in the best position to provide information on which vulnerabilities, if any, have been tested and found to be exploitable or not.

SBOM Details

A SBOM is a machine-readable list of the components in a piece of software. Fortress uses the data from SBOMs to inform on areas of risk, such as potential vulnerabilities, outdated components, presence of code contributions from adversarial countries, license information, as well as checks on malware, and component integrity.
A Vulnerability Exploitability eXchange (VEX) is a machine-readable companion document to an SBOM which explains if a product is affected by a discovered vulnerability. VEXs explain if a potential vulnerability is exploitable in a product and why.

The requested fields for these documents are based on standards developed by from the National Telecommunications and Information Administration (NTIA), National Institute of Standards and Technology (NIST), and Cybersecurity and Infrastructure Security Agency (CISA).

Complete depth may not always be feasible, especially as SBOM practices are still new to many companies. When an SBOM cannot convey the full set of components, it should explicitly acknowledge the “known unknowns,” so consumers can easily determine the difference between a component with no further dependencies and a component with unknown or partial dependencies.

To provide the most accurate analysis of a product’s components, we ask that certain data fields be included in an SBOM and VEX files. The table below includes standard data fields to include, but is not limited to:

SBOM Data Field	Description
Metadata	
Timestamp of the SBOM	The exact time that the SBOM was generated. A timestamp is an unambiguous way to remove confusion about which version of an SBOM is being referenced.
Author or Tool Which Made the SBOM	The people or tools which created the SBOM document
Product Data	
Product Name	Name of the product that is the subject of the SBOM.
Product Supplier Name	Supplier of the product that is the subject of the SBOM.
Product Version	Version string for the product that is the subject of the SBOM.
Product Identifier	A unique product identifier, specifically a specifically a Common Platform Enumeration (CPE), a Package URL (PURL), or both.
Product Type	For example: device, application, library, framework, service, container image, file, firmware, or operating system.
Product Description	Short description of the product and/or features.
Product Licenses	License information on the product.
Cryptographic Hash of the Product File	For example, SHA-256, SHA-1, or MD5 hash of the software package.
Download Location of the Product File (Typically a URL)	A URL where the product can be downloaded.
Component Data (Per Component)	
Component Name	Common name by which the component is known.
Component Supplier Name	Supplier name for the component. For an open-source component this may be the name of the project.
Component Version	Component version string.
Component Identifier, specifically a Common Platform Enumeration (CPE) or a Package URL (PURL), or Both	Common Platform Enumeration (CPE) is a standardized method of describing and identifying classes of applications, operating systems, and hardware devices. A Package URL (PURL) can be used to uniformly identify and locate a software package across programming languages, package managers, packaging conventions, tools, APIs, and databases.
Component Type	For example: device, application, library, framework, service, container image, file, firmware, or operating system.
Component Description	Short description of the component and/or features.
Component Licenses	The license(s) which apply to the component.
Download Location of the Component	A URL of where the component was downloaded.
Cryptographic Hash of the Component	For example, SHA-256, SHA-1, or MD5 hash of the software package.
Version Control System Location	Typically, a GitHub or similar URL for open-source components to track and manage changes to files over time.
Component Relationship Information	The relationships between components, as well as between a component and the product itself. For example, a relationship of “depends on” can describe how components are dependent on other components in the product.

VEX Data Field	Description
Metadata	
Timestamp of the VEX	The exact time that the VEX was generated. A timestamp is an unambiguous way to remove confusion about which version of an SBOM is being referenced.
Author or Tool Which Made the VEX	The people or tools which created the VEX document.
Product Data	
Product Name	Name of the product that is the subject of the VEX.
Product Supplier Name	Supplier of the product that is the subject of the VEX.
Product Version	Version string for the product that is the subject of the VEX.
Product Identifier	A unique product identifier, specifically a specifically a Common Platform Enumeration (CPE), a Package URL (PURL), or both.
Exploitability Data	
Vulnerability Identifier	Typically, a Common Vulnerabilities and Exposures (CVE) number or GHSA ID.
Vulnerability Description	A description of the vulnerability as provided by the source.
Exploitability Status	Lists if the product is affected by the vulnerability. For example, “not_affected.”
Remediation Information	Details on how to handle or fix a vulnerability, if available.

What’s Next?

Once the SBOM is uploaded and analysis is completed, you may request a copy of the report, which will be provided to you in the vendor portal.

As products are updated, new versions released, you may be asked to provide the SBOM for the new version(s).