Solution Brief

SBOM as a Prioritization Method for Log4j Software Vulnerability

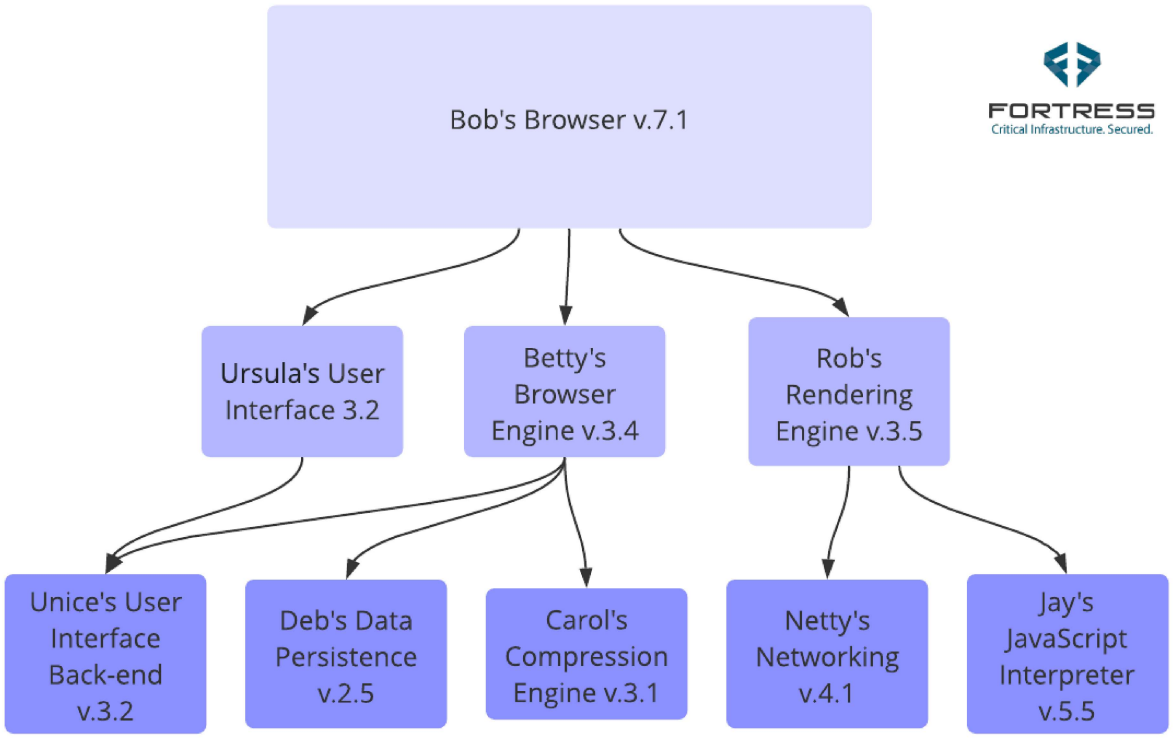
December 11, 2021

File Integrity & Software Assurance Solution

Fortress proposes to utilize the File Integrity & Software Assurance (FIA) solution to answer the question facing security teams trying to determine their exposure to known vulnerabilities. By utilizing a software analysis approach that results in both a software bill of materials (SBOM) as well as analysis of that SBOM, whilst confirming software source and integrity, software suppliers and consumers alike can obtain visibility into likely candidates of vulnerable software.

What is an SBOM?

An SBOM is an inventory of components found in a software product, along with metadata and dependency relationships for those components. Think of it like the list of ingredients on a box of breakfast cereal. You want to know that the software is good for you or won't harm you. But for decades, software consumers have been using software with zero visibility into what's inside the products they depend on for safe food processing, power generation, office productivity, big data processing, and yes, the internet at large. This lack of transparency, combined with the advent of a digital transformation that has brought software to the nexus of every important part of our lives, is the core issue that prompted the need for SBOMs in the first place.



SBOMs should be machine readable and processed using automation. While they can be read by humans, the sheer volume of data from multiple updates per year across hundreds of thousands of software packages in a typical organization would greatly overwhelm most of us. Software is dynamic and changes frequently, and if our software component inventory grows stale, then the insights about that inventory will also be similarly flawed. They can come in many formats, but most

commonly in JSON or XML documents, or in the case of some tool vendors, proprietary formats.

Using SBOMs for Vulnerability Management

Most software users have grown accustomed to the idea they can trust the supplier of their software to discover vulnerabilities in their product and develop patches for them. The idea is that vulnerabilities can be neutralized with a patch in a relatively short amount of time. An example is Microsoft's monthly patches to its Windows operating system. In theory, the situation should be no different when it comes to vulnerabilities in components. Whenever a new vulnerability is identified in a component in their product, the supplier should develop a patch for it. If for some reason the supplier is unable to develop a patch right away, they should have private discussions with customers regarding alternate steps the customer can take, for example, isolating the affected devices from the rest of the network, pending availability of a patch.

What about Vulnerability Scanners?

The problem is that vulnerability scanners cannot identify these issues, and so an SBOM is needed to identify potential vulnerabilities. Vulnerability scanners are designed around the concept of writing a specific plugin for a specific vulnerability, and with hundreds of thousands of vulnerabilities in the National Vulnerability Database, the scanner vendors cannot hope to have tests for all of them. For instance, Tenable Security Center, otherwise known as ACAS in the defense space, only has plugins for 66,412 CVE in the NVD that contains over 160,000 vulnerabilities with new ones every day. That's less than 42% coverage.

Additionally, even when the scanner vendor writes a plugin, they only cover one specific instance of that vulnerability. In the case of the Apache Log4j vulnerability CVE-2021-44228, there are 4 separate Tenable plugins looking for very specific implementations of this vulnerability, however there are tens of thousands of ways this vulnerability can be implemented given the ubiquitous nature of this component. Not to mention this requires a credentialed scan and in large enterprises, many assets cannot be scanned with credentials. The only reliable and scalable way is with an SBOM.

Fortress File Integrity & Software Assurance (FIA) Solution: Process Overview

1. Fortress obtains a list of software to be analyzed and other information as requested below and onboards the list of monitored software into FIA.
2. Fortress ingests the target software and produces a resultant software assessment report and SBOM highlighting the vulnerable components.
    - Software assurance activities include the creation of a software bill of materials and vulnerability analysis to identify known vulnerabilities.
        - Based upon SBOM findings, Fortress can provide a Vulnerability Exploit Report (VEX) for potentially vulnerable software and prioritize the response. Fortress will provide results in both machine readable and human readable formats documenting the results of the analysis and recommended mitigations.
    - Fortress also validates software authenticity and integrity including all patches and updates for target software. Authenticity checks include checking the supplier for

known breaches, appropriate encryption delivery, updated security certificate and DNS checks. Integrity checks include reviewing code signage, malware analysis and in some cases sandbox and firmware analysis.

3. Fortress works with the customer through Fortress internal tool sets, or the customer's own workflow, to track and manage the risk and remediation process through initial finding until closure.
4. Fortress will then onboard the target software for continuous monitoring for similar risks as supported in the FIA solution as an annual subscription.
5. Fortress will check the software daily over the subscription period and notify customer of results, including notification that new software and patches are available.
6. Fortress will provision client tools that allow for bulk analysis of files to determine if they have been previously assessed and the outcomes of that analysis.

Assumptions

- Customer will provide the following information:
  - Name of software and version to be monitored
  - Location of where software is to be obtained
  - Credentials required to download the software if it is behind a supplier paywall. Credentials are securely shared via Fortress secure portal
  - Credentialed products may only be shared with customer who provided the credentials
  - Point of contact to be notified of any software risks. There may be different points of contact for each software under monitoring
- SBOM results are considered to be a potential finding, and not evidence of exploitability. SBOMs will dramatically reduce the level of effort and result in a prioritization mechanism allowing customer to eliminate possible vulnerable software so that verification efforts are only performed on a subset of software.
- VEX verification will only be performed on potentially vulnerable software identified by SBOMs and only after mutual agreement with customer and Fortress.

Solution Brief

Critical Apache Log4j Vulnerability

www.fortressinfosec.com

Fortress Information Security, LLC
1.855.FORTRESS
189 S. Orange Avenue
Orlando, FL 32801