Supplemental Project Notice

OPERATIONALIZING SOFTWARE BILL OF MATERIALS (SBOMS)

Yes, we have the software bill of materials!

PROJECT HIGHLIGHTS

- Building an SBOM Program
- Understanding inventory details and how to approach vendors about aquiring SBOMs
- How to evaluate SBOM quality and perform vulnerability analsysis
- How to approach exploitability analysis to prioritze SBOM findings

Background, Objectives, and New Learnings

Energy delivery infrastructure consists of numerous control systems that contain a combination of standalone software applications and devices with embedded software ("control system software"). In contrast to traditional IT networks, operators cannot easily conduct active vulnerability scans on this infrastructure due to the potentially disruptive side effects. Additionally, much of the software is embedded in proprietary devices, where there is a lack of access to conduct internal monitoring or vulnerability assessments. Due to these limitations and recent, high-impact supply chain security issues, including the Log4Shell vulnerability and the Solarwinds supply chain attack, the energy sector has kicked off multiple initiatives to increase supply chain transparency. By exchanging Software Bills of Materials (SBOMs), all stakeholders in the software supply chain are able to understand which 3rd-party software components, and thus 3rd-party vulnerabilities, are present in control system software.

While the SBOM initiative will dramatically improve software supply chain visibility, transparency, and vulnerability notification efforts, they are note simple. Understanding of inventories, difficulty getting vendors to provide SBOMs for equipment, and then the daunting task of prioritizing vulnerabilities identified make starting an SBOM program no small lift. By collaborating with other utilities in this process though, and sharing learnings on the most effective ways to overcome these challenges, the hope is to elevate the industry and provide more insight into the software used throughout the electric industry than ever before.

Commercially available binary Software Composition Analysis (SCA) tools can automatically generate an SBOM and correlate vulnerabilities; however, this approach tends to lead to many false positive vulnerabilities. These vulnerabilities may impact the component but are not present, reachable, or exploitable within the context of the as-built software, system, configuration, or network environment. As SBOM efforts gain traction, gaining insight into exploitability and how to prioritize specific vulnerabilities will be more and more important.

Benefits

Utilities that participate in this project will have the foundation of a SBOM program, and will understand what inventory details are necessary, how to approach vendors about SBOMs for devices, how to analyze the vulnerabilities presented by those SBOMs and how to approach an exploitability analysis to determine priorities.

Additionally, utilities will benefit from the Automated Device Vulnerability Exploitation and Defensive Impact Analysis (ADVEDIA) DOE DE-FOA-0002500 project developing new insights into vulnerability and exploitability analysis.

Project Approach and Summary

The project involves five main tasks:

Task 1 – Generate Inventory of devices and software inside predetermined scope, such as a substation.

Task 2 – Request SBOMs from vendors for identified inventory and track results.

Task 3 – Verification and Validation will be done through testing of devices and software and comparing to vendor provided SBOMs. The purpose of this is to see if the vendor provided SBOMs appear to be complete.

Task 4 – Analyze vulnerabilities and risks, looking at trends, categorization, etc.

Task 5 – Exploitability Analysis involving Vulnerability Exploitability eXchange (VEX) and other methods

Deliverables

- A Technical Report that presents findings and recommendations for the funders based on the analysis conducted across the industry on the success, challenges, and opportunites invovled with operationalizing SBOMs.
- An individual report with:
  - The acquired inventory
  - Available SBOMs
  - Verification analysis
  - Vulnerability and Exploitability analysis

Price of Project

The price to join this project is $125,000 per utility. Funding qualifies for self-directed funding (SDF).

Project Status and Schedule

The project schedule is approximately 18 months depending on the availability of the participant's resources and facilities.

Who Should Join

Utilities that want to understand how to effectively create a program to utilize to capture and utilize SBOMs.

Contact Information

For more information, contact the EPRI Customer Assistance Center at 800.313.3774 (askepri@epri.com).

Technical Contact

Ben Sooter at 865.218.8108 (bsooter@epri.com)

Technical Advisor Contact Information

Central: Chuck Wentzel at 618.320.0011 (cwentzel@epri.com)

Northeast: Anne Haas at 704.608.6314 (ahaas@epri.com)

Southeast: Barry Batson at 704.595.2879 (bbatson@epri.com)

West: Brian Dupin at 650.906.2936 (bdupin@epri.com)

Product ID: 3002031084 **Project ID:** 01-120171 **April 2025**

EPRI
3420 Hillview Avenue, Palo Alto, California 94304-1338 • USA • 800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com