INL/MIS-25-83332-Revision-0

Energy Sector SBOM and HBOM Quarterly Working Group - February Presentation

February 2025

Robert J Erbes, Lucas Tate

Changing the World's Energy Future

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/MIS-25-83332-Revision-0

Energy Sector SBOM and HBOM Quarterly Working Group - February Presentation

Robert J Erbes, Lucas Tate

February 2025

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

U.S. DEPARTMENT OF ENERGY | *Office of* Cybersecurity, Energy Security, and Emergency Response

DOE CESER

Energy Sector SBOM and HBOM Quarterly Working Group

FEBRUARY 19, 2025 | 2PM - 3PM EST | VIRTUAL EVENT

Presented by Robert Erbes (INL) and Lucas Tate (PNNL)

INL/MIS-25-83332

Overview

- BOMs *could* become an enabling technology for *supply chain risk management*
- We identified several “key challenges” that prohibit SBOM usage at scale
- We’re actively developing research activities to help move toward solving these problems

KC1. Associating a CVE with a product does not mean it's vulnerable

- CVE correlation is not the finish line.
- Investigations take time and resources.
- Efforts to mitigate a vulnerability that was either never present in the first-place or not exploitable costs time and money.

- Notable Efforts
  - VEX
  - CSAF
  - Automated Device Vulnerability Exploitation and Defensive Impact Analysis (ADVEDIA)

KC2. What should be shared between OEMs and Asset Owners? How can that be done most effectively?

- There is a common sentiment in the SBOM community, that SBOMS need to be shared and that this will improve security.
- How do SBOMs compare to existing practices?
- Where should the responsibility of supply chain security fall?
- What information is useful? to whom? and when? And how can it be efficiently exchanged?
- What are the tangible benefits in the most idealistic scenarios?

- Notable Efforts
  - A SBOM'd Substation (Southern Company)

KC3. Dealing with the heterogeneity of SBOMs

- Software naming has always been a difficult problem.
- The standards leave a lot of room for interpretation, which leads to variability.
- Variability inhibits speed and scalability.

- Notable Efforts
  - Data Normalization Challenges and Mitigations in Software Bill of Materials (SBOM) Processing [1]
  - SBOM Harmonization Plugfest 2024[2]

[1] https://www.mitre.org/sites/default/files/2024-10/PR-24-2647-Data-Normalization-Challenges-Mitigations-Software-Bill-Of-Materials-Processing.pdf
[2] https://resources.sei.cmu.edu/news-events/events/sbom/

KC4. Toward understanding the “quality” or “suitability” of SBOMs

- Does the information in the SBOM satisfy the intended use case?
- Did the author do a good job?

- Notable Efforts
  - Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM) [1]
  - SBOM Operations Working Group (DHS CISA SBOM Community)

[1] https://www.cisa.gov/sites/default/files/2024-10/SBOM%20Framing%20Software%20Component%20Transparency%202024.pdf

KC5. Acknowledging SBOM types

- Design / Source / Build / Analyzed / Deployed / Runtime
- The assumptions and use cases depend on which SBOM type is being utilized.
- What's best? Should they all exist?

- Notable Efforts
  - Types of Software Bill of Materials (SBOM) [1]

[1] https://www.cisa.gov/resources-tools/resources/types-software-bill-materials-sbom

KC6. How should BOMs be mapped to products?

- Sometimes software is the end-product and subsequently we may understand how or where a vulnerability in Windows 10 might affect us.
- In other cases, it might be quite difficult to intuit all the software/firmware embedded in a device you use every day.
- If a vulnerability is released for an embedded software/firmware, it can be difficult to point to all the affected devices.
- We need ways to describe how BOMs relate to specific products and systems.

KC7. What new challenges arise from enterprise-scale BOM management

- Much research into the theoretical or realized utility of BOMs relies on small, curated data sets.
- This is not a good surrogate for thousands or millions of products being actively updated and patched.
- Need more work to explore how scale impacts BOM vulnerability management processes.

What's Next?

- Feedback on the key challenges
  - Are they the right ones?
  - We did some work to vet them, but the space is constantly shifting.

- Planned Activities
  - **KC1. Associating a CVE with a product does not mean it's vulnerable**
    - Document describing the challenges that is geared toward individuals who don't have a lot of experience in remediating vulnerabilities.
  - **KC2. What should be shared between OEMs and Asset Owners? How can that be done most effectively?**
    - Collaborative effort with industry

Thank You

@DOE_CESER

linkedin.com/company/office-of-cybersecurity-energy-security-and-emergency-response

energy.gov/CESER

U.S. DEPARTMENT OF ENERGY | *Office of* Cybersecurity, Energy Security, and Emergency Response