ETSI The Standards People

Security Conference

Software Bill of Materials (SBOM)

Presented by: Phyllis Lee, VP of Content Developent

CIS Center for Internet Security®

16/10/2023

SBOM Demand

US National Policy

- Executive Order 14028: Improving the Nation's Cybersecurity
  - Section 4: Enhancing Software Supply Chain Security
    - *" (vii) providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website;"*
- US National Cybersecurity Strategy
  - References EO 14028 and SBOMs
  - Strategic Obejective 3.3: *Shift Liability for Insecure Software Products and Services*
    - *"…promote the further development of SBOMs;"*

SBOM Demand cont'd

- Federal Food, Drug, and Cosmetic Act, Section 524B, "Ensuring Cybersecurity of Devices" requires medical devices containing software that connects to the internet to provide an SBOM that includes data on commercial, open-source, and off-the-shelf software components
- EU Cyber Resilience Act stresses the importance of SBOM (Article 37)
  - *"A software bill of materials can provide those who manufacture, purchase, and operate software with information that enhances their understanding of the supply chain, which has multiple benefits, most notably it helps manufacturers and users to track known newly emerged vulnerabilities and risks. It is of particular importance for manufacturers to ensure that their products do not contain vulnerable components developed by third parties."*

SBOM Demand cont'd

- Australian Cyber Security Centre, "Information Security Manual: Guidelines for Software Development", Australia, 2022
- Canadian Forum for Digital Infrastructure Resilience Supply Chain Assurance Working Group, "Recommendations to Improve the Resilience of Canada's Digital Supply Chain", Canada, 2022
- National Cyber Security Center (NCSC), "NCSC Issues Fresh Guidance Following Recent Rise in Supply Chain Cyber Attacks," United Kingdom, 12 October 2022

Benefits of an SBOM

- Software Inventory
- Details of components of a software package
- Keep software up-to-date
- Vulnerability in a software component
- Software Licensing
- Machine Readable
  - Integrate into existing tools
  - Query for vulnerabilities
  - Automated patching

SBOM – Minimum Elements for USG

Data Fields

- Supplier Name
- Component Name
- Component Version
- Other Unique IDs
- Dependency Relationship
- Author of SBOM Data
- Timestamp

SBOM – Minimum Elements for USG

Automation Support

- Software Package Data eXchange (SPDX)
- CycloneDX
- Software Identification (SWID) tags

SBOM – Minimum Elements for USG

Practices and Processes

- Frequency: update SBOM with new build or release
- Depth: Minimum, all top-level dependencies must be listed with enough detail to seek out the transitive dependencies recursively
- Known Unknowns: data should affirmatively state when the direct dependencies of a component have been fully enumerated, or when a component has no further dependencies.
- Distribution and Delivery: available in timely fashion and must have appropriate access permissions
- Access Control: provider gets to decide how public/private SBOMs are. It must be specified up front and could vary depending upon sw licensing
- Accommodation of Mistakes: allow for omissions and errors

SBOM Generation and Consumption

Generation

- Ask Suppliers for SBOMs
  - Update Contracts
- How to share?
  - Access Control
- For Latest Software Releases

Consumption

- Ask Suppliers for SBOMs
  - Update Contracts
- How to receive/ask?
  - Updates/Patches

Vulnerability Management

- Vulnerability Exploitability eXchange (VEX)
  - Security advisory to indicate of component of software package is vulnerable
    - Under Investigation, Fixed, Known Affected, or Known Not Affected
  - Works with SBOM
- Common Security Advisory Framework (CSAF)
  - Predecessor to VEX
  - Fixed, Not Affected
  - VEX is a profile in CSAF
- VEX not supported by all organizations

VEX

Advantages

- Software vendor responsible for providing vulnerability information
- Push vs. Pull

Disadvantages

- Software vendors hesitant to support due to false positives
- End organizations update software packages outside of software vendor support

CIS Tools Support SBOMs

- CIS Controls Self Assessment Tool (CSAT) Pro and CIS Configuration Assessment Tool (CAT) Pro
- CycloneDX
- Included in installer package and available for download on WorkBench

Conclusion

- SBOMs are coming!
- Don’t let perfection be the enemy of progress.
- “Minimum Elements” will have to grow to fully realize the promise of an SBOM