Framing

NTIA Software Supply Chain Transparency

January 13, 2021

Framing Working Group

Managed with love and patience by co-chairs Michelle Jump and Art Manion

Meeting almost weekly since July 2018

- Fridays at 1400 EDT
- https://lists.sei.cmu.edu/mailman/listinfo/ntia-sbom-framing

Framing concepts that apply to the entire multi-stakeholder process

Michelle Jump

MedSec LLC

Global Regulatory Advisor - Medical Device Cybersecurity

MichelleJump@medsec.com

Art Manion

Software Engineering Institute
CERT Coordination Center

Principle Engineer “/” Technical Manager

amanion@cert.org

Agenda

1. SBOM refresher
2. New draft documents – finalizing comment resolution
    1. Sharing and Exchanging SBOMs
    2. Software Identification Challenge and Guidance
3. Expected upcoming work
    1. “VEX”
    2. Glossary
4. Considerations for Further Work
    1. Beyond baseline
    2. Integrity/Authenticity/Provenance

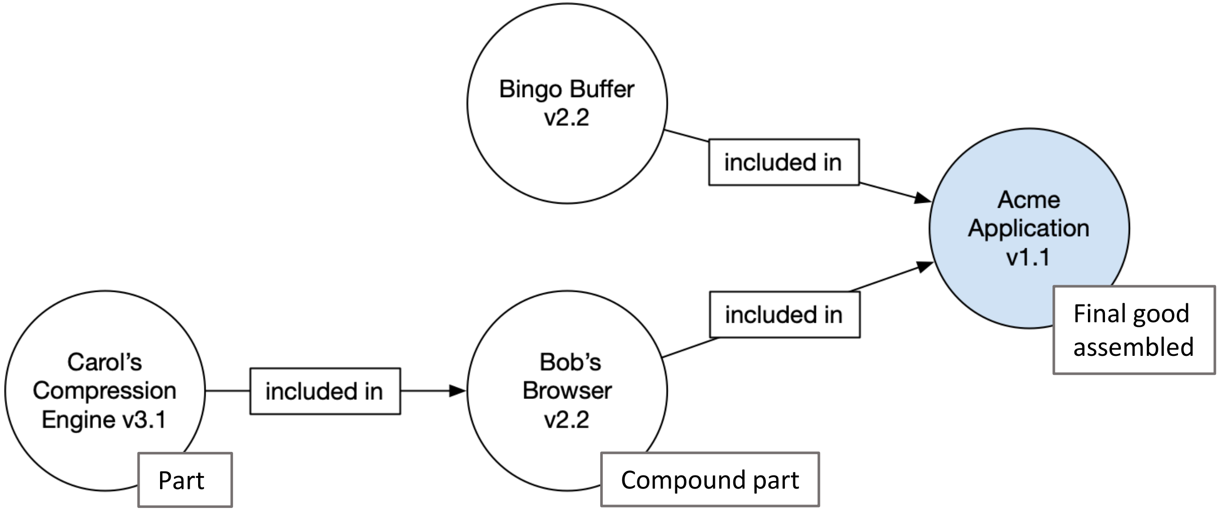
Refresher: What is an SBOM?

Framing Software Component Transparency: Establishing a Common Software Bill of Material (SBOM)

https://tinyurl.com/y7s8ab3t

"An SBOM is effectively a nested inventory, a list of ingredients that make up software components."

Partial Table of Contents



Component Name	Supplier Name	Version String	Author	Hash	UID	Relationship
Application	Acme	1.1	Acme	0x123	234	Self
|--- Browser	Bob	2.1	Bob	0x223	334	Included in
|--- Compression Engine	Carol	3.1	Acme	0x323	434	Included in
|--- Buffer	Bingo	2.2	Acme	0x423	534	Included in

Two Discussion Papers
Sharing
Identity

Final Review of Two Draft Papers

Thank you for the feedback. Finalizing last of updates.

1. Draft paper: Sharing and Exchanging SBOMs
   - https://tinyurl.com/y3cbn9zs

2. Draft paper: Software Identification Challenge and Guidance
   - https://tinyurl.com/y6pnhvke

Draft paper: Sharing and Exchanging SBOMs

> "Transparency in the supply chain enables better risk decision-making for producers and consumers of software. This means that information about the underlying software components in a piece of software—a Software Bill of Material (SBOM)—should be accessible to the right entities at the right time."

Draft paper: Software Identification Challenge and Guidance

> "Possibly the biggest single challenge to supply-chain transparency and the SBOM model is the difficulty in identifying software components globally... This paper captures some of the major challenges… and offers some guidance on how to address these challenges."

Ongoing Efforts

Framing: Key Issues Going into Phase II

- **Is the baseline accurate and effective?**
    - Healthcare Proof of Concept asked to test it out

- **What do you call it?**
    - Inconsistencies cause traceability issues. Both supplier and component names can vary. Windows vs Win, etc

- **How do you share it?**
    - No central SBOM database so how do you ensure availability?

- **What if its not exploitable?**
    - An SBOM is not the full story. “VEX” addresses status of a specific vulnerability

Two Ongoing Efforts

Framing Group Focus on two primary efforts

1. VEX
   - Vulnerability exploitability status

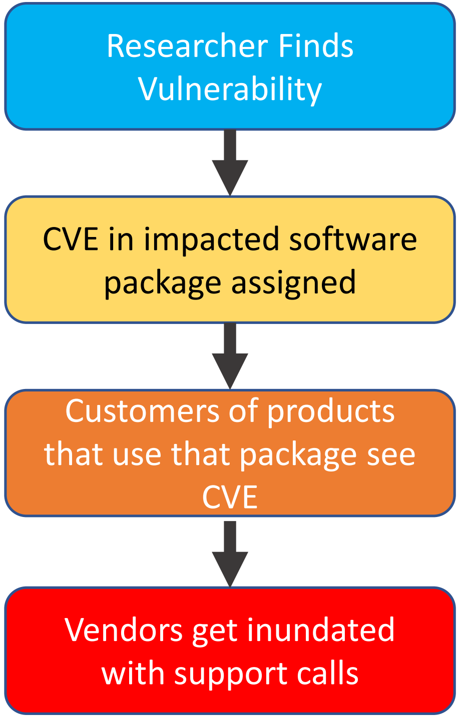
2. Glossary
   - Common set of terms

“VEX:” Vulnerability (or exploitability) status

- To date has been called “VEX” (Vulnerability EXploitability)
  - Ironic that we’re having trouble with names?
  - The name is up for discussion
- Step 1: Draft description of the problem, needs, use cases
  - I see a vulnerable upstream component, what is my exposure?
  - https://tinyurl.com/yx8qvma7
- Step N: Solve problem
- Need to map vulnerability to component exists outside of SBOM

VEX: Problems we set out to solve

- Customers can **sometimes** see what packages are installed
- They can’t see whether the package has been fixed
- They don’t know if their devices are vulnerable or if their environments are exposed
- Downstream developers want to know whether their software providers applied a fix



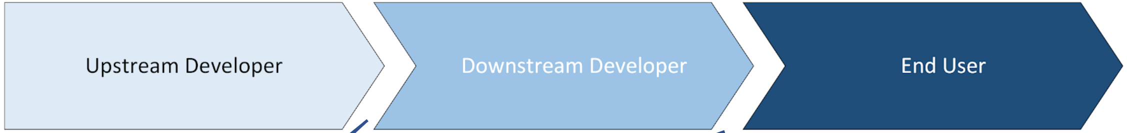
Researcher Finds Vulnerability

CVE in impacted software package assigned

Customers of products that use that package see CVE

Vendors get inundated with support calls

VEX: Draft business requirements



Upstream Developer

- Delivers components for use by others.
- Creates CVEs
- May create SBOMs

Downstream Developer

- Consumes and utilizes components created by others.
- May deliver a product to the end user or another downstream developer
- Creates CVEs
- Consumes upstream CVEs
- May create SBOMs
- May indicate Product vulnerability to upstream vulnerabilities
- Wants to minimize end user calls for non-affected Products

End User

- Makes use of the Product
- Consumes CVE, SBOM, and VEX information
- Desire to understand their risk exposure
- Desire to minimize false positive vulnerabilities.

Interfaces

Information elements

VEX: What we’ve been doing, and next steps

- We have a draft business requirements document
- Examining different formats
  - CycloneDX
  - CVRF from CSAF
- We think integrity checks and attestation are key components
- The binding between VEX and SBOM is the index which is a name

Next Steps

- We’re going to continue discussions with CSAF to see if we can use CVRF to meet our requirements
  - We can also test our business requirements as we have those discussions

Parking Lot

- As two discussion papers are wrapping up, Framing is reviewing other Phase I parking lot items
  - One particular focus area: **Moving beyond the minimum: expanding the baseline SBOM**
  - During creation of the baseline SBOM, Phase I report outlined that restricting the SBOM to these elements would limit use cases.
  - Framing will be looking at expanding the elements to describe other information that could be added to the SBOM and how that expands the use cases possible
  - Also**: Integrity/authenticity/authority, provenance**