SBOMs are Dropping Now What?

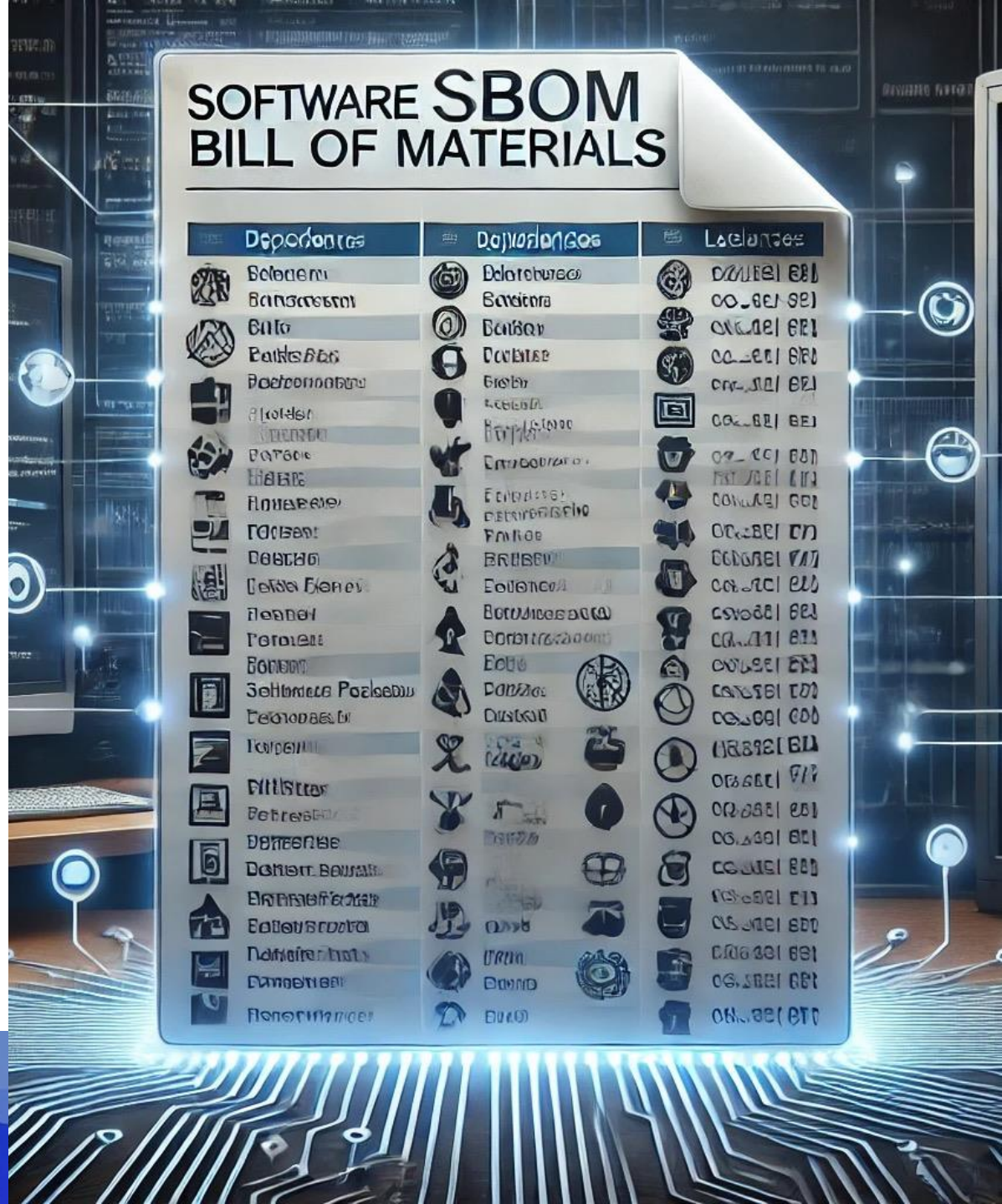
Grab Your Towel and Don’t Panic

Michael F. Angelo
Distinguished Technologist
Open Text

James McQuiggan
Cyber Security Advocate
KnowBe4

Agenda

- Quick History
- SBOM what you get
- How to look at an SBOM
- What to do with the result



Quick History

- Solar Winds - Pushed issues with Supply Chain
  - Regulatory, Legislative, Standards, and Customers
    - i.e. NIS-2, DORA, EO 14028, ISO 15408, CISA (Attestation and Pledge), 2023 SEC (impact all companies and as a provider for technology), OMB requirements
- Log4J
  - Where is it?
  - Is it vulnerable?
  - Is it even being used?
- What about XZ, polyfill.io… Ugh

Minimum SBOM - NTIA

Data Field	Description
Supplier Name	The name of an entity that creates, defines, and identifies components.
Component Name	Designation assigned to a unit of software defined by the original supplier.
Version	Identifier used by the supplier to specify a change in software from a previously identified version.
Other Unique Identifiers	Other identifiers that are used to identify a component, or serve as a look-up key for relevant databases
Dependency Relationship	Characterizing the relationship that an upstream component X is included in software Y
Author of SBOM Data	The name of the entity that creates the SBOM data for this component.
Timestamp	Record of the date and time of the SBOM data assembly.

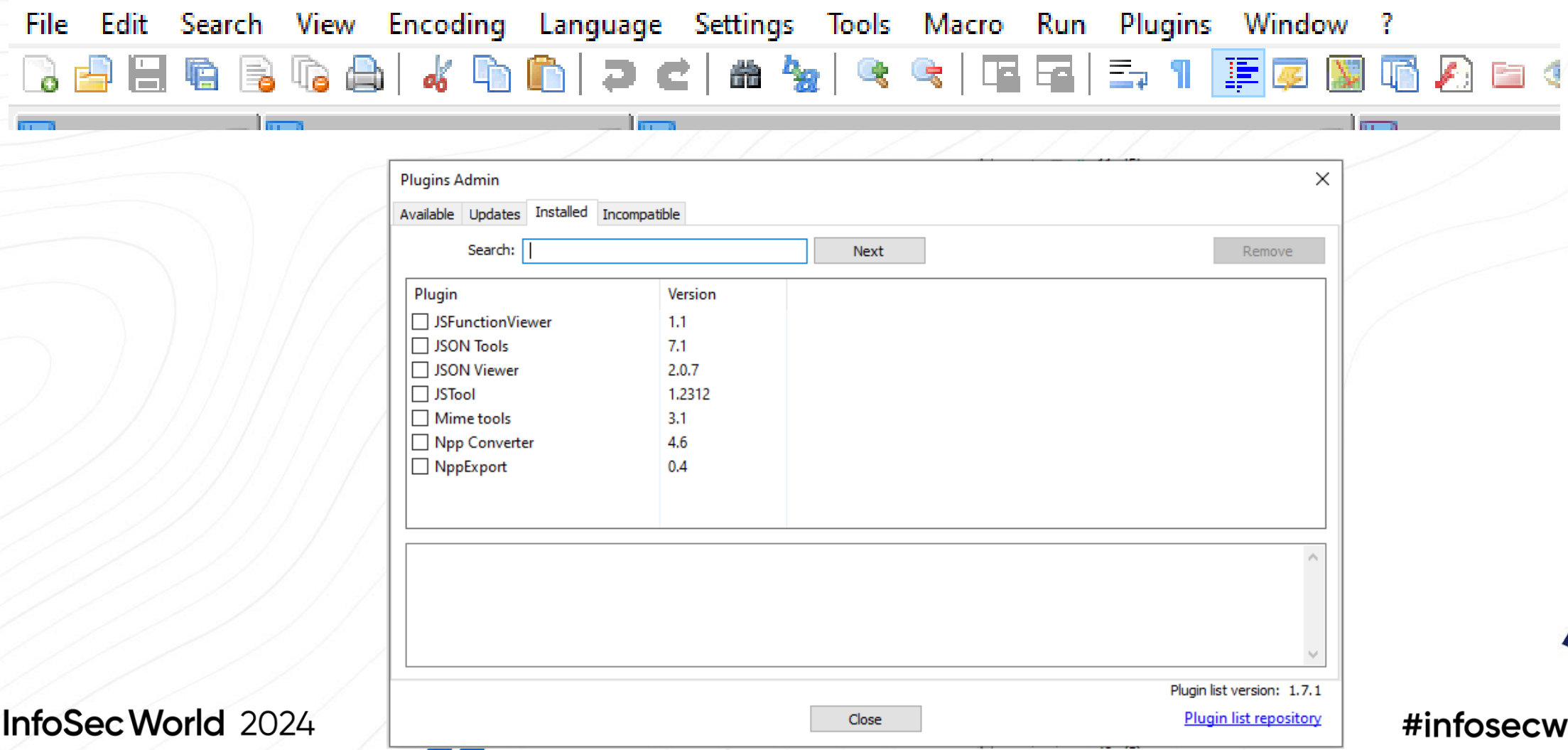
SBOM – What You Get

- Machine Readable
- SBOM Contents
  - Must include all components (Open Source and Commercial)
  - Does not include company defined components
- BTW
  - List all CVEs… top level
- And we really want to see if product has vulnerable components

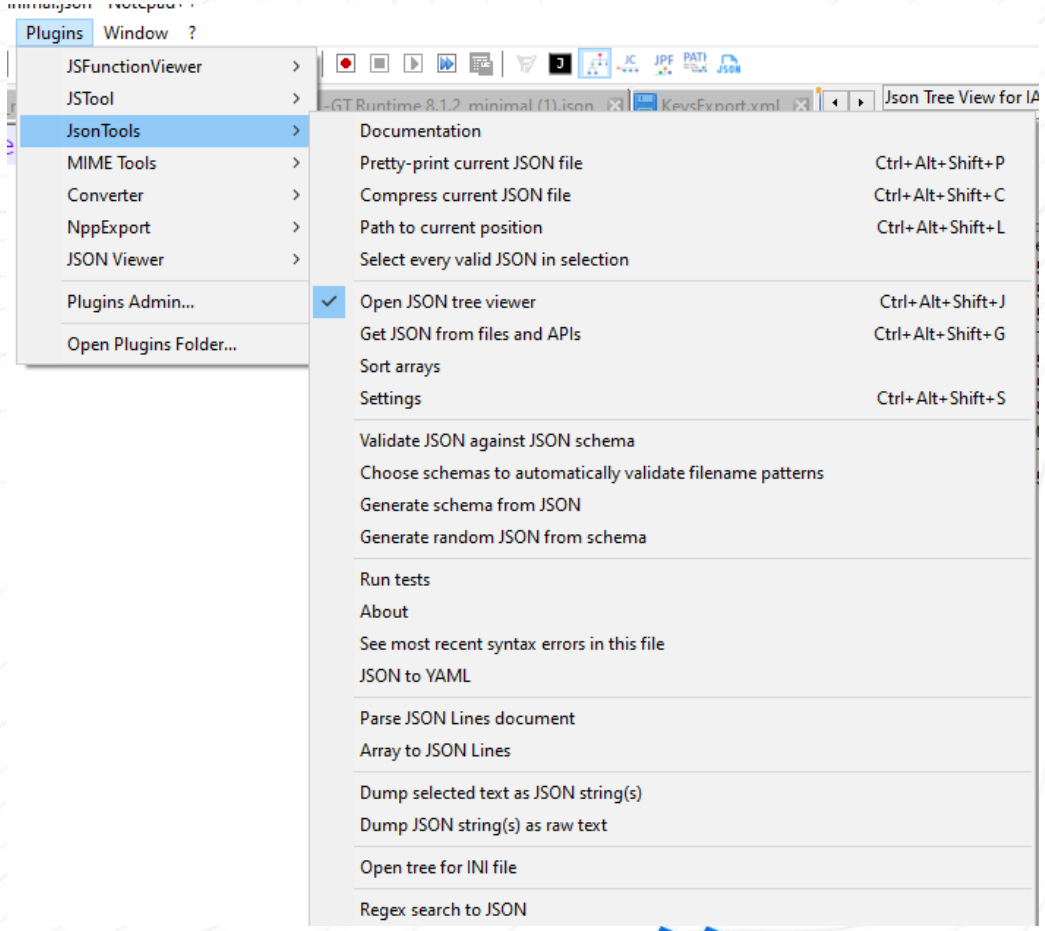
Sample CycloneDX

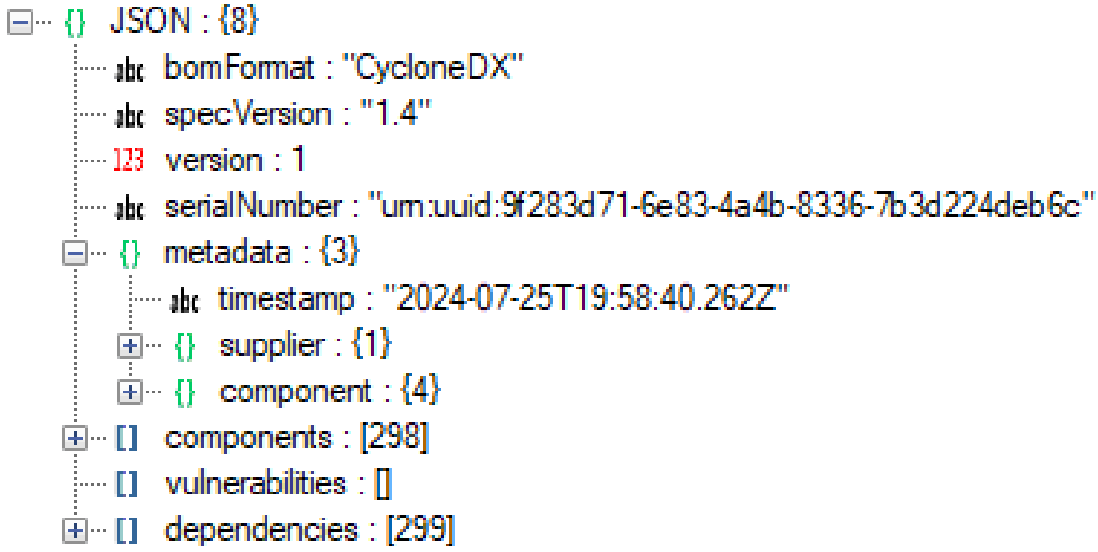
- "bomFormat":"CycloneDX","specVersion":"1.4","version":1,"serialNumber":"urn:uuid:8826f786-17a1-4784-be95-5f7e51a04dd9","metadata":{"timestamp":"2024-08-02T21:27:45.860Z","supplier":{"name":"OpenText"},"component":{"type":"application","name":“Product Name","version":"24.3.0 (Bundle+)","bom-ref":"66b151ce-6caa-4d53-ab11-2b6651e8401e"}},…
- Really hard to read..

NotePad++


File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
Plugins Admin
Available Updates Installed Incompatible
Search:
Next
Remove
Plugin
Version
JSFunctionViewer 1.1
JSON Tools 7.1
JSON Viewer 2.0.7
JSTool 1.2312
Mime tools 3.1
Npp Converter 4.6
NppExport 0.4
Plugin list version: 1.7.1
Close
Plugin list repository

NotePad ++


Plugins
Window
?
JSFunctionViewer
JSTool
JsonTools
MIME Tools
Converter
NppExport
JSON Viewer
Plugins Admin...
Open Plugins Folder...
Documentation
Pretty-print current JSON file Ctrl+Alt+Shift+P
Compress current JSON file Ctrl+Alt+Shift+C
Path to current position Ctrl+Alt+Shift+L
Select every valid JSON in selection
Open JSON tree viewer Ctrl+Alt+Shift+J
Get JSON from files and APIs Ctrl+Alt+Shift+G
Sort arrays
Settings Ctrl+Alt+Shift+S
Validate JSON against JSON schema
Choose schemas to automatically validate filename patterns
Generate schema from JSON
Generate random JSON from schema
Run tests
About
See most recent syntax errors in this file
JSON to YAML
Parse JSON Lines document
Array to JSON Lines
Dump selected text as JSON string(s)
Dump JSON string(s) as raw text
Open tree for INI file
Regex search to JSON
Json Tree View for IA


{} JSON : {8}
bomFormat : "CycloneDX"
specVersion : "1.4"
version : 1
serialNumber : "urn:uuid:9f283d71-6e83-4a4b-8336-7b3d224deb6c"
{} metadata : {3}
timestamp : "2024-07-25T19:58:40.262Z"
{} supplier : {1}
{} component : {4}
[] components : [298]
[] vulnerabilities : []
[] dependencies : [299]

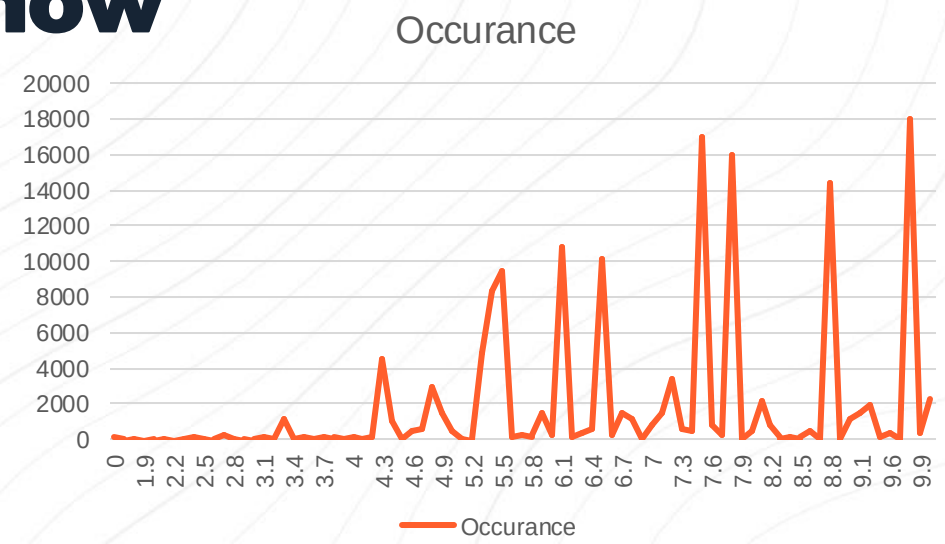
Lots of Other SBOM Materials & Tools

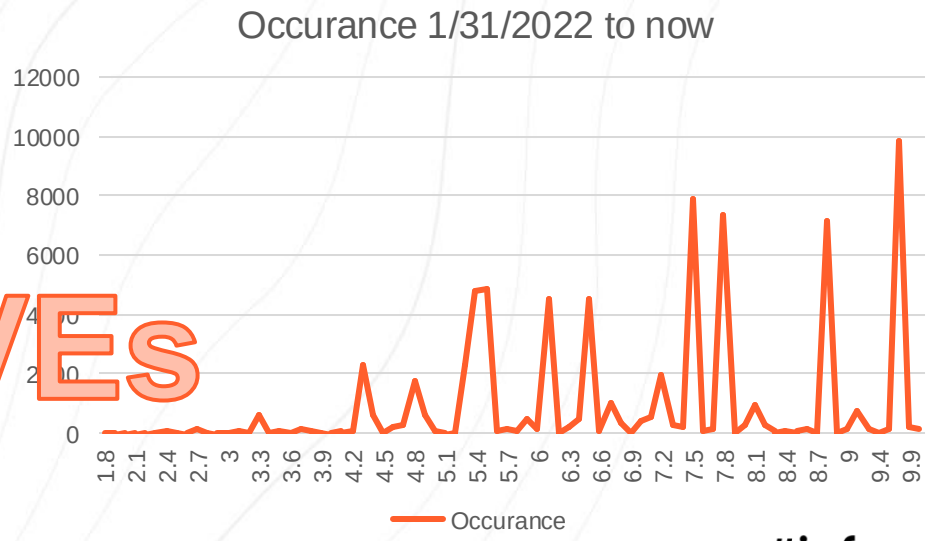
- Great Article - SBOM in Action: finding vulnerabilities with a Software Bill of Materials
- Look for Open Source Vulnerabilities (OSV) database
  - https://osv.dev/
- Free Tools
  - https://github.com/anchore/syft
  - https://github.com/anchore/grype
  - https://github.com/aquasecurity/trivy

SBOMs...
How bad can it be??

CVE Statistics – 2017 to now

0	73	4.4	1032	7.2	3427
1.2	3	4.5	60	7.3	535
1.8	6	4.6	483	7.4	439
1.9	4	4.7	623	7.5	17032
2	7	4.8	2939	7.6	784
2.1	61	4.9	1424	7.7	242
2.2	19	5	500	7.8	15913
2.3	55	5.1	62	7.9	30
2.4	158	5.2	44	8	479
2.5	52	5.3	4828	8.1	2178
2.6	16	5.4	8346	8.2	748
2.7	185	5.5	9418	8.3	154
2.8	21	5.6	100	8.4	176
2.9	18	5.7	254	8.5	133
3	6	5.8	228	8.6	496
3.1	108	5.9	1488	8.7	50
3.2	21	6	220	8.8	14414
3.3	1132	6.1	10782	8.9	6
3.4	26	6.2	116	9	1100
3.5	180	6.3	362	9.1	1477
3.6	35	6.4	601	9.3	1938
3.7	163	6.5	10087	9.4	75
3.8	73	6	[illegible]	[illegible]	[illegible]
3.9	51	7	[illegible]	[illegible]	3
4	115	8	[illegible]	[illegible]	[illegible]
4.1	82	6.9	58	9.9	340
4.2	110	7	813	10	2227
4.3	4474	7.1	1477		





149116 CVEs

Statistics – since 8/28/2024

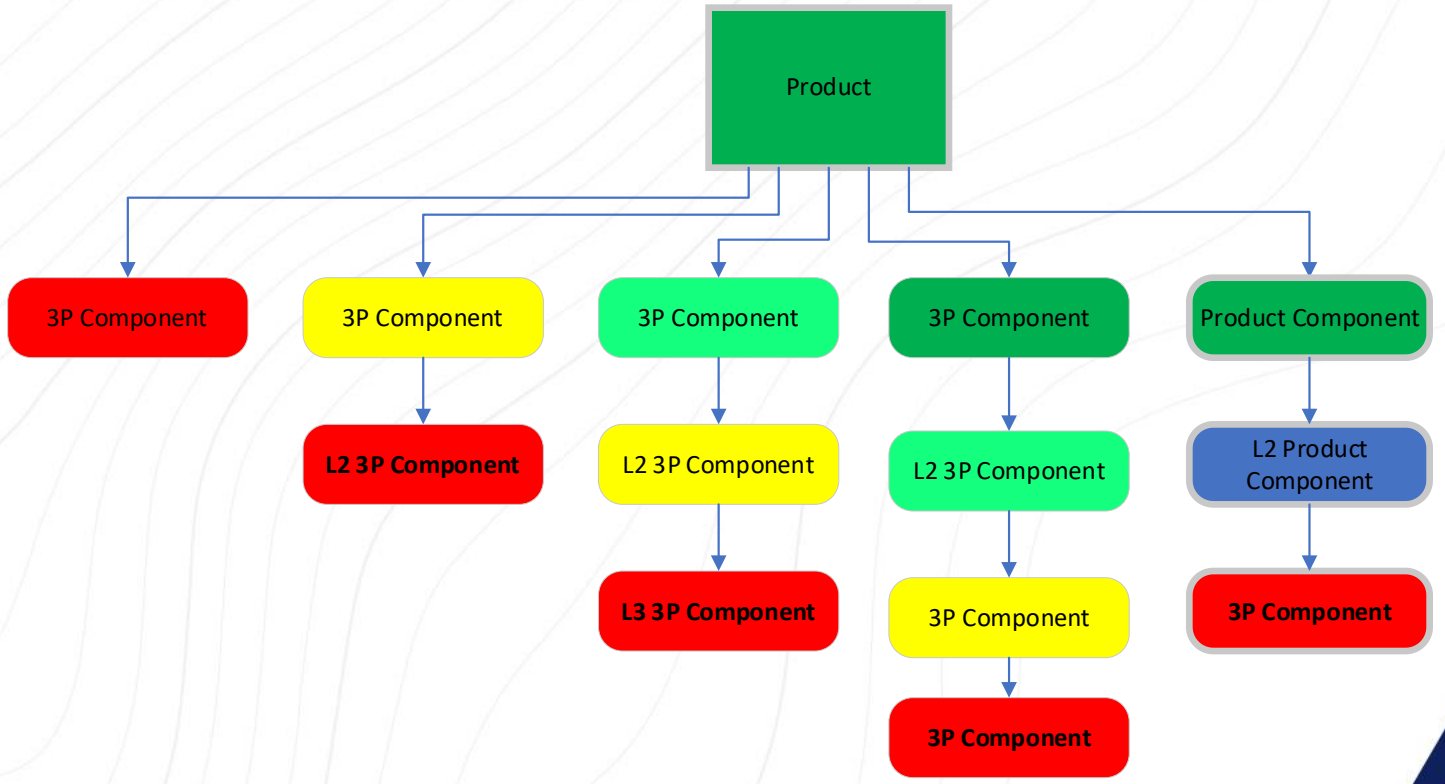
- 200 products + components
- 63638 components used in products
  - De-duplicated - 1692 components
  - 211 Components - 1166 CVEs
  - 121 Critical & Highs
- The numbers sound bad, but the target landscape reduces, however still not good…

You have an SBOM.... Handling Strategy


DON'T
PANIC

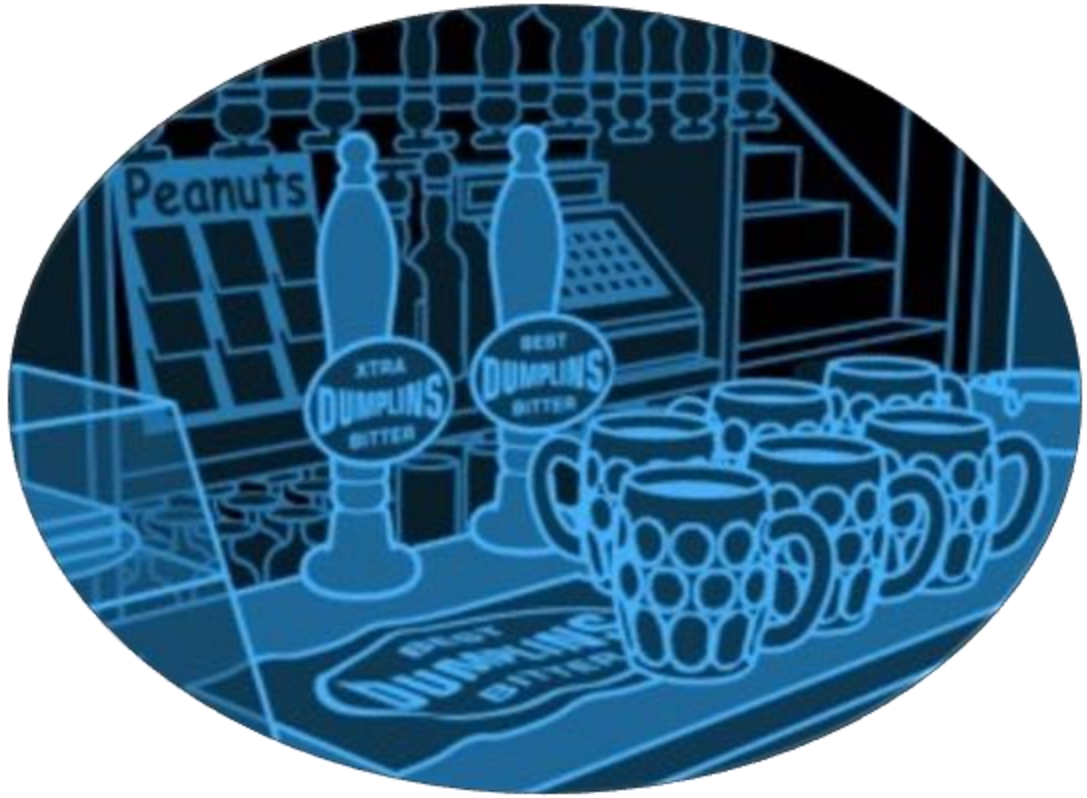
SBOM Layout Simple

- L0 – Product
  - L1a – Component in Product
  - L1b – Another component
    - L2[a-z] – Components in L1b
      - L3[a-z] – Components in L2b
- SBOM may not contain L2 or L3



Remember…

- Don’t think of SBOMs as a galactic targeting system, but as a defense mechanism – or a way to justify head count.
- Don’t Panic, Drink 6 pints at the local pub, and know where your towel is…



Issues: Product Appears to Have Old CVEs

Product A

- Was released Feb 2024

What you see

- SBOM lists Component A
- Component A has CVE-2016-2123

What you should do

- Read the CVE – confirm the Component Version is Impacted.
- Check the last update date on the CVE
- Look for a VEX record
- Ask the provider to confirm that the CVE is not impacting.
- Reality check – an 8 year old CVE is probably not impacting.

Issues: Was CVE in product prior to release

Item

- SBOM Contains component CVE YYYY-######

Issue

- Did not address CVE in product or product does not have a VEX record

Thing to check

- CVE's may be reserved before the product is released, and then closed after product release.
- Causes appearance that product shipped with a know CVE.
- Check to see the last update date in CVE record

Issues: Does CVE have CVSS >= [Critical | High]

Item

- SBOM Contains component with a critical or high CVSS (>=7)

Issue

- Product may not release with a critical or high CVSS

Thing to check

- Same as before
- CVSS can be modified after filing.
- Check history.

Issue: Product was accepted, now a new CVE

Item:

- SBOM expansion shows CVE in component.

Issues:

- Product has apparent vulnerability.

Things to Check:

- Is component in use?
- Can component be accessed?
- Lots of Open-Source is bloated.
- Various deserialization attacks exist.

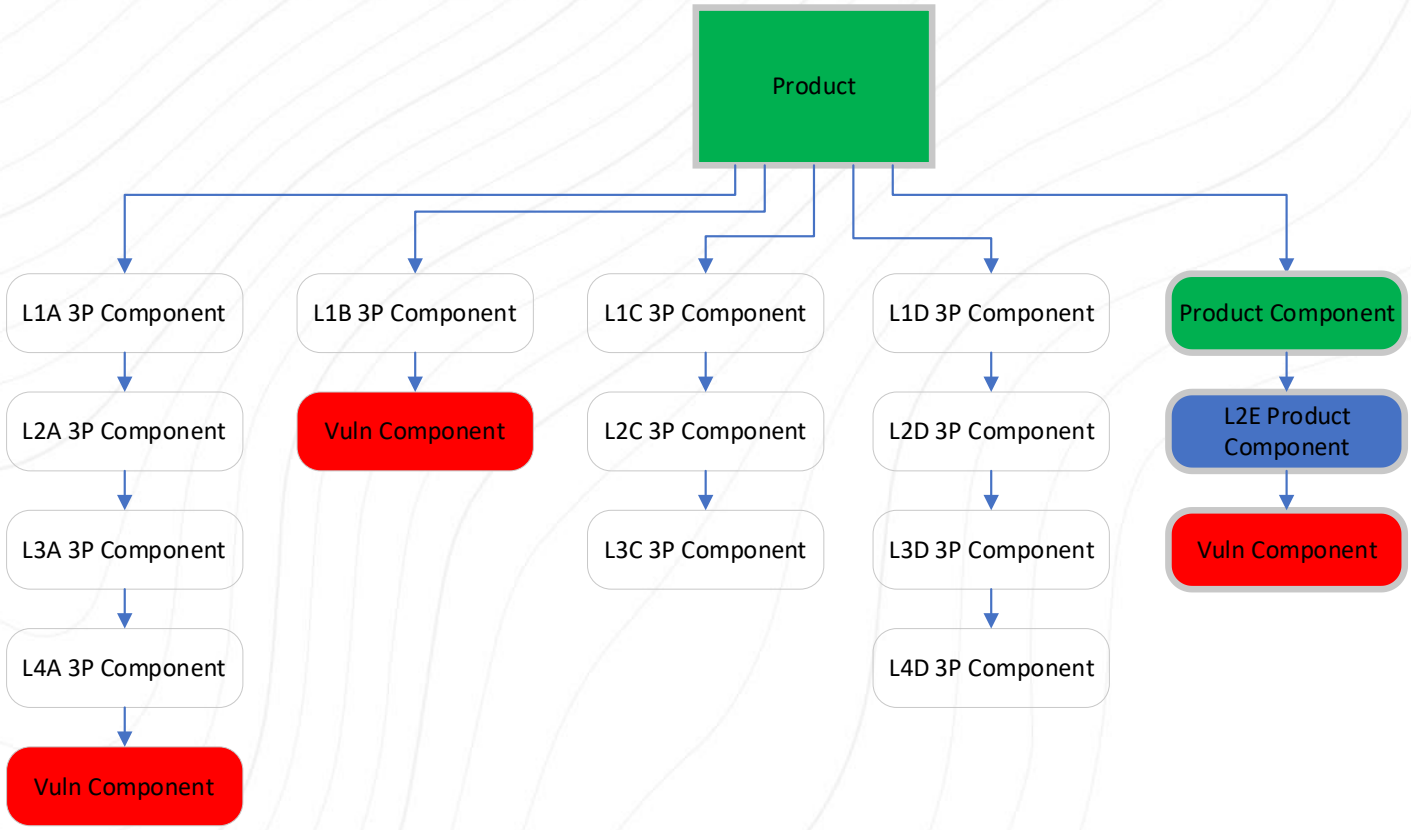
Things to Consider

- Before we move on…
- Do you trust the vendors (and their answers) or not?
  - If not… Why…
- CVEs are not static.
  - Component CVEs can be updated at anytime.
    - Years after being reserved.
  - Component CVEs can be created at anytime.
    - Even after a product is released.

Transitive Dependencies

Item

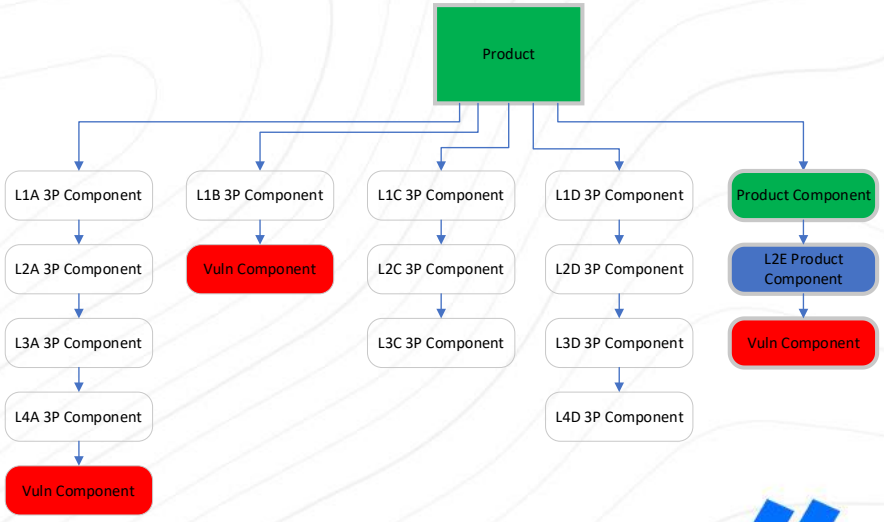
- SBOM expansion shows CVE 3 levels down.



Transitive Dependencies

Item

- SBOM expansion shows CVE 3 levels down.



Issues

- You don't know how to tell if you are impacted.
- Who do you look to for fix?

Things to Check

- CVSS score
- Nature of issue.
- Can CVE be realized?

Things to Consider

Item:

- Published SBOM has Component A,
- SBOM for A has Component B1
- SBOM Scan shows Component A with B3 or No B

Issues:

- SBOM doesn’t match calculated SBOM.

Things to Check:

- Is B3 newer than B1?
- Are there vulns in B1 that B3 addresses?
- Was B removed as it isn’t being used?

More to Consider

- SBOM :
  - Discovery Tools will content to evolve
  - Reporting Tools will continue to evolve
  - Attacks against systems via SBOMs will continue to evolve
  - Defenses enabled using SBOM information will continue to evolve

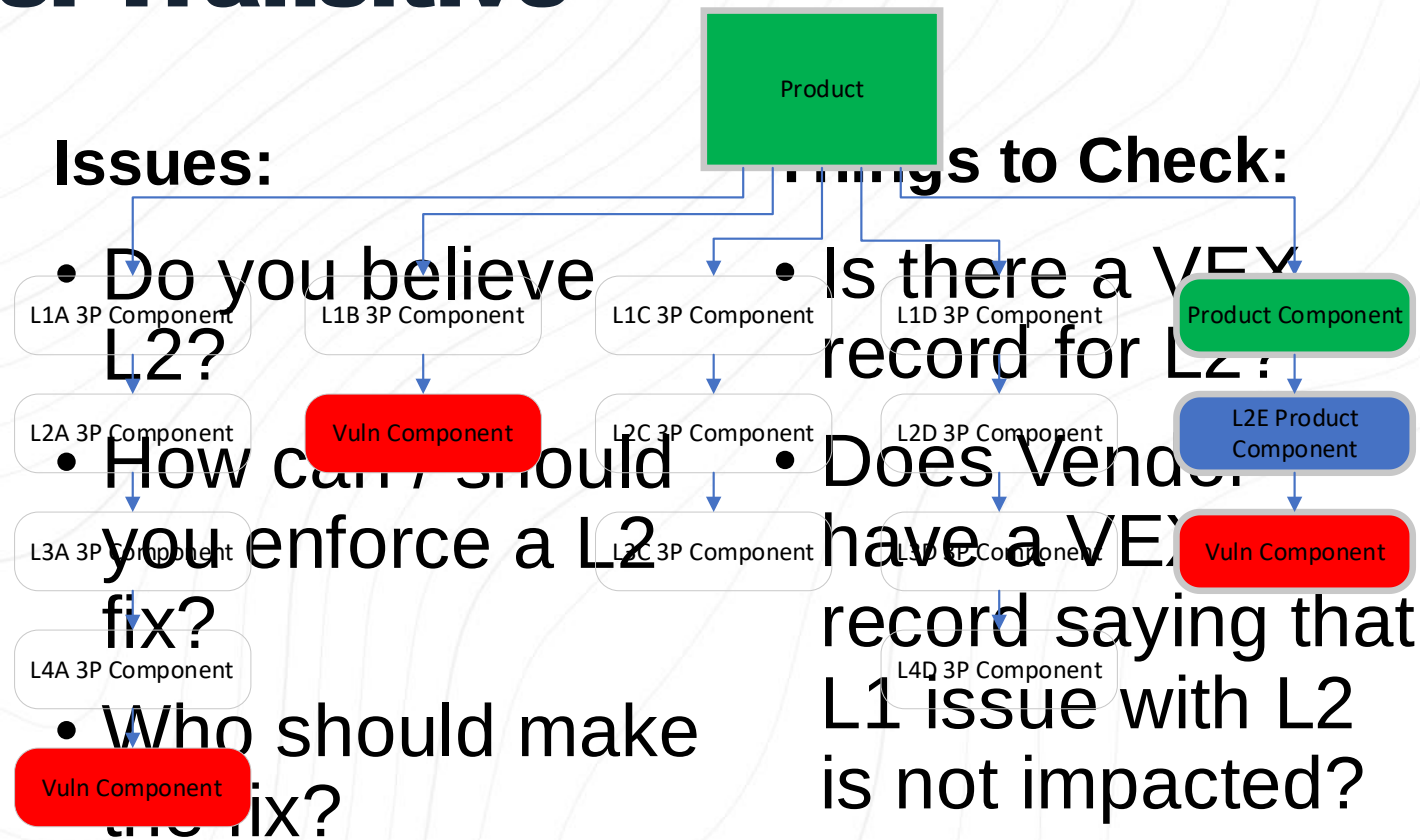
Advanced Issues: Transitive

Item:

- SBOM expansion shows CVE 3 levels down.
- Component @ Level 2 says it is not an issue

Issues:

- Do you believe L2?
- How can/ should you enforce a L2 fix?
- Who should make the fix?



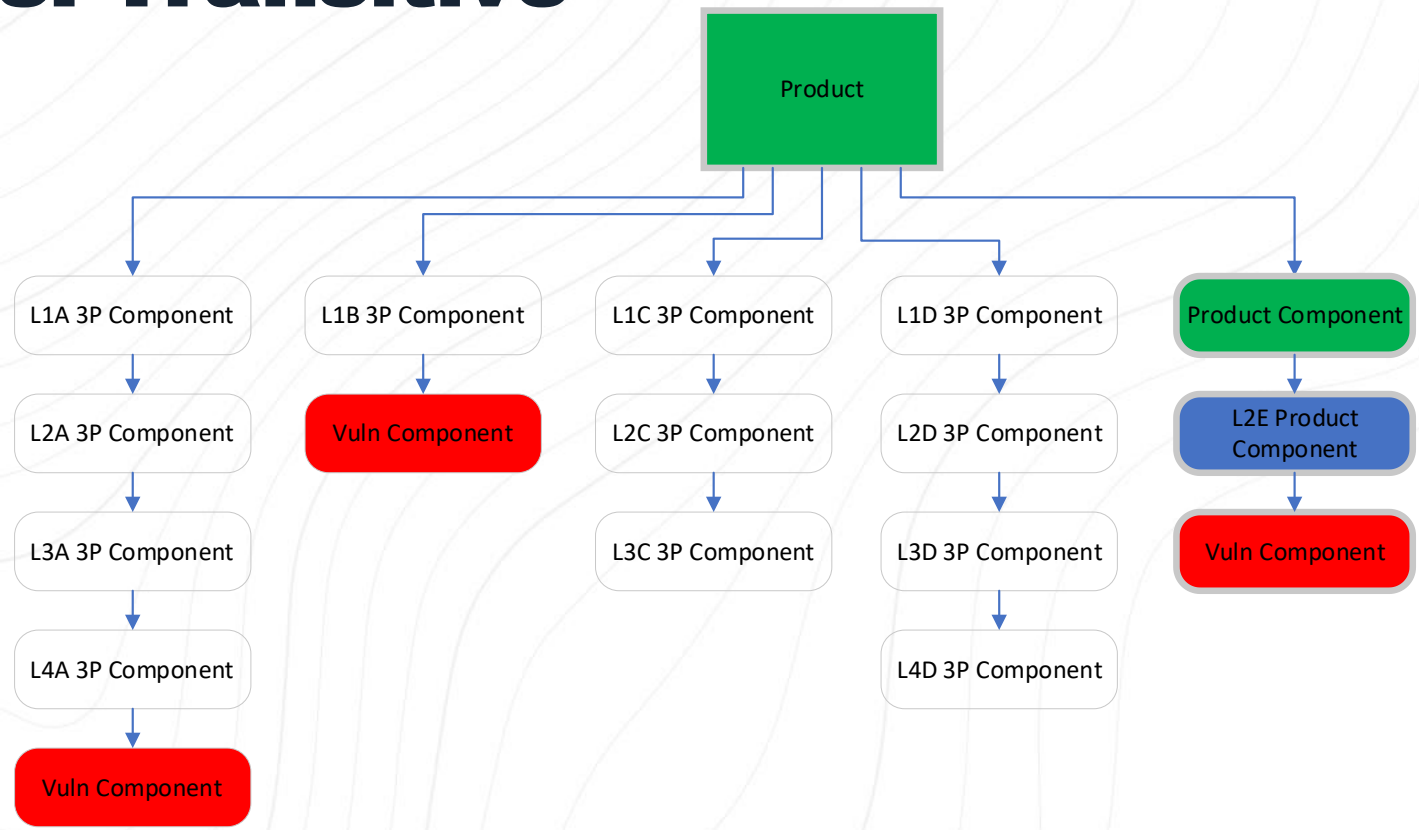
Things to Check:

- Is there a VEX record for L2?
- Does Vendor have a VEX record saying that L1 issue with L2 is not impacted?

Advanced Issues: Transitive

Item:

- SBOM expansion shows CVE 3 levels down.
- Component @ Level 2 says it is not an issue



Advanced Issues: Transitive

Item

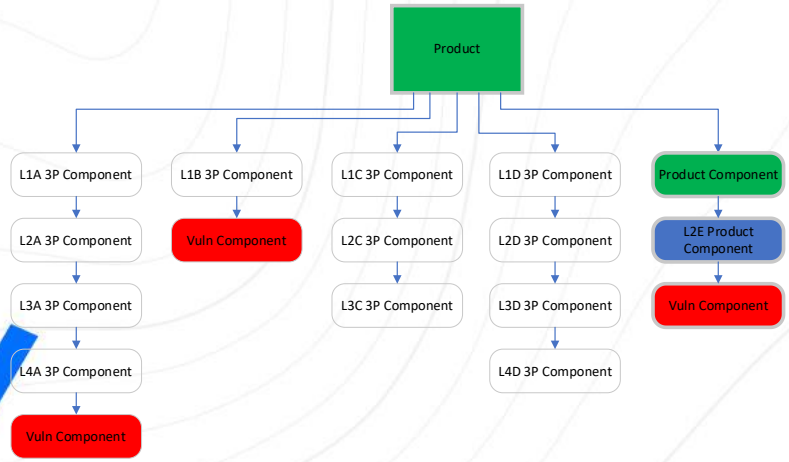
- SBOM expansion shows CVE 3 levels down.
- Component @ Level 2 is no longer supported

Issues:

- Should Product owner update L2?

Things to Check:

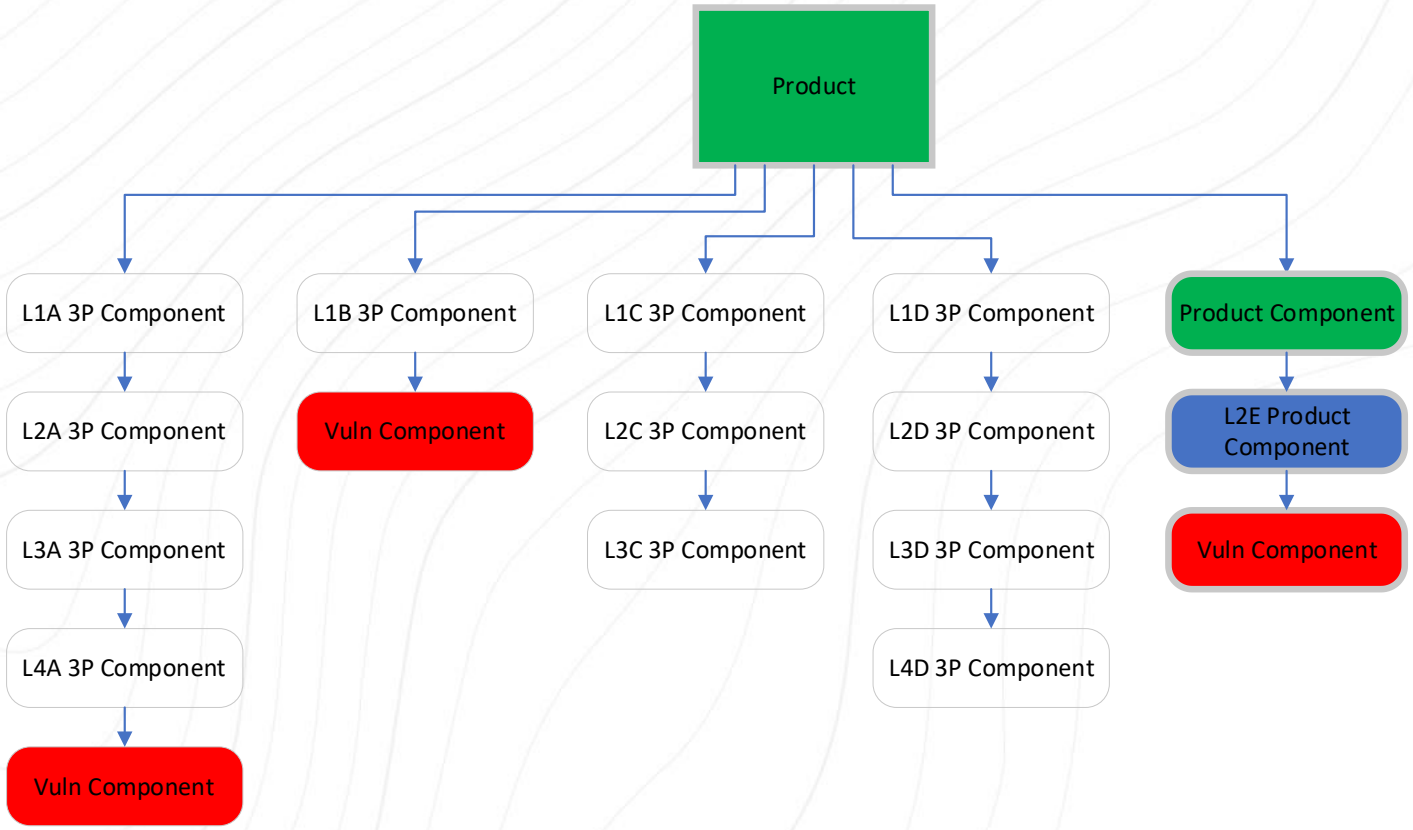
- Does L2 have a newer version which is supported?
- Is L2 accessible in your environment?



Advanced Issues: Transitive

Item

- SBOM expansion shows CVE 5 levels down.
- Component @ Level 4 is updated, but does not declare a CVE



Advanced Issues: Transitive

Item

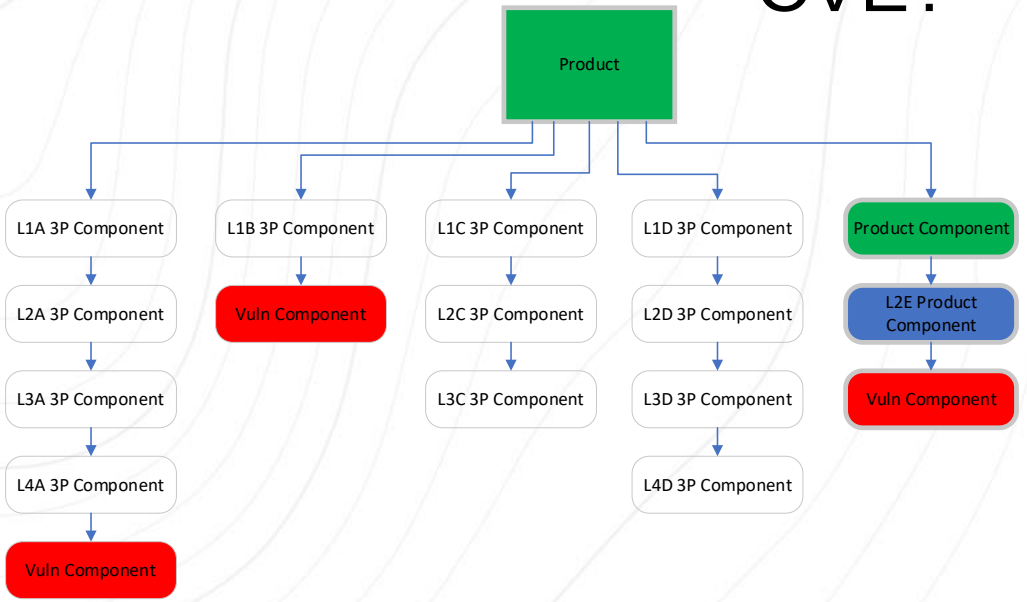
- SBOM expansion shows CVE 5 levels down.
- Component @ Level 4 is updated, but does not declare a CVE

Issues:

- Do you need to upgrade?

Things to Check:

- Did they change the component that had the CVE?



Advanced Issues: Transitive Discrepancies

Item

- You receive Vendor SBOM, and run your own tool.
- SBOMs do not match.

Issues:

- SBOMs should represents what is in the product.

Things to Check:

- SBOM discover tools are still evolving.
- Are the identified components newer than what the tool says?
- Products may update components

Advanced Issues: Transitive

Item

- Your tool that generates cascaded transitive SBOMs (based on other SBOMs)
- Does not match Vendor SBOM.

Issues:

- Vendor may upgrade transitive elements and declare them in their SBOMs
- Cascaded SBOMs may have old information

Things to Check:

- Are the vendor components newer than the cascaded?
- Products may update components and cascaded may not reflect them.
- Top version numbers may stay same if not provided by component owner.

Advanced Issues: Old Components

Item:

- SBOM contains 4000 parts, and 90% are > 2 years old

Issues:

- Is someone still maintaining the component?
- Is CVE reporting still occurring?

Things to Check:

- Is there a newer version of the component?
- Have there been any vulnerabilities?
- Have they been fixed?

Advanced Issues: EoL Components

Item:

- SBOM contains 2 EoL Components

Issues:

- An EoL component is not monitored for CVEs. (No way to report it).

Things to Check:

- Has the component ever had a vulnerability?
- Is there a replacement component?
- Is the vendor paying for extended support?
- Ask the vendor about impact.

Bottom Line Why You Care…

Market Impact	External Impact
SEC fines (not final) • Consent decree against company • Consent decree against CEO / CISO	Regulatory: • EO 14028 – mandates SDL & SBoM • NIS-2 / DORA Standards: • ISO 15408 Extensions
Class Action Lawsuit • $26M	Customers: • OMB – Required SBoM for sales to Government & Critical Infrastructure • US encouraging consumers 'No SBoM' discount.
Stock: • 25% drop in 2 days, 35% within month • Before Event: 23.48 • After Event: low $7.72 • 3 Years later – Today: 11.58	Government Sales Requires: • CISA Pledge • Attestation

AI... SBOMs
WMD or Galactic Defender

Not SBOM… AIBOM

- Elements of AIBOM – algorithms, data sources
- Managing vulnerabilities – 3rd party sources
- Ethical / Legal Compliance
- Maintenance / Updates
- Using AIBOM for customers / transparency

AI & SBOMs – Things to Consider

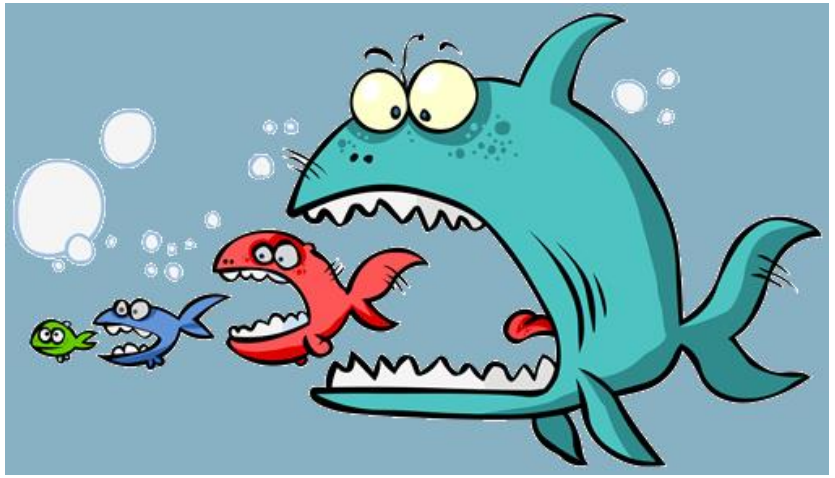
- Can I use AI to create my SBOM?
- Should I post all the vulnerabilities
- Can it show me the software with XYZ?
- Can I use AI to get me active / passive reconnaissance
- Can I use AI to run the penetration test?

Things to do and consider

- Trust the vendors (and verify their answers).
- Not all fixes require code – Admin or Procedural
- CVEs are not static.
  - Component CVEs can be updated at anytime.
    - Years after being reserved.
  - Component CVEs can be created at anytime.
    - Even after a product is released.

Last Thoughts

- Not all is bad as it looks
- Not all mitigations need to be in code – i.e. procedural.
- Sometimes Component updates, to address CVEs require additional component updates which should be taken into consideration.
- Pay attention to insurance / Liability
  - Beware of SEC issues.



Special Thanks

- Tom Incorvia – for working diligently for past 20 years on supply chain and for putting up with my sense of irony
- Mark Vaszary, PHD candidate – for his input, comments, and giggle testing along the way.

THANK YOU!