PUBLIC SUBMISSION

As of: June 19, 2021
Received: June 17, 2021
Status: Pending_Post
Tracking No. kq1-1fim-1bak
Comments Due: June 17, 2021
Submission Type: Web

Docket: NTIA-2021-0001
Software Bill of Materials Elements and Considerations

Comment On: NTIA-2021-0001-0001
Software Bill of Materials Elements and Considerations

Document: NTIA-2021-0001-DRAFT-0007
Comment on FR Doc # 2021-11592

Submitter Information

Name: Sandy Carielli
Address:
MA,
Email: scarielli@forrester.com

General Comment

Thanks for the invitation to comment on Software Bill of Materials Elements and Considerations. Here are some comments for your consideration:

• Section (3)(i) Vulnerabilities:
o This is an important point: “the existence and status of vulnerabilities can change over time, and there is no general guarantee or signal about whether the SBOM is up-to-date relative to all relevant and applicable vulnerability data sources.” The SBOM is not the place to track vulnerabilities. As noted, vulnerabilities in components can be discovered at any time, and while it is pretty straightforward to tie an SBOM version to a software version, it will be more difficult to ensure that you have the most up-to-date version of the SBOM if you have to keep revising it for every new vulnerability in the product.
o We have other tools to track and manage vulnerabilities in software. Rather than relying on the SBOM itself to hold that information, ensure that software composition analysis (SCA) and vulnerability risk management (VRM) tools support the latest SBOM formats (most SCA tools support at least one format today or plan to do so). Then encourage organizations to leverage those tools to map known vulnerabilities to the components in the SBOM. This will enable a more real-time view of how vulnerabilities in components can impact software.
o The other risk of including vulnerabilities in the SBOM is articulated in (3)(j): a vulnerability in a particular component in a piece of software may not be exploitable in that piece of software, either because no active exploit exists (though this could change), or because the vulnerability is not part of a call path in the software (aka, it is not reachable). Without proper prioritization as to which vulnerabilities were included in an SBOM, we risk distracting security leaders with unreachable vulnerabilities.

• Section (3)(j): Risk Management:
o As mentioned above, it’s not uncommon for software to be unaffected by a vulnerability in a component due to that vulnerability not being reachable (the vulnerable part of the code is never called). When new

vulnerabilities are discovered, it will be important for suppliers to communicate whether that vulnerability is reachable in their product (referred to in the RFC as Vulnerability Exploitability eXchange, or VEX). The notion of a VEX makes sense but adding VEX information into the SBOM itself is risky (again, exploitability can change).

Thanks, and best regards,

Sandy Carielli
Principal Analyst, Security & Risk
Forrester Research