Request for Public Comment on Software Bill of Materials - NowSecure Response

NowSecure, Inc. (parent company viaForensics, LLC)
1608 Spring Hill Rd, Ste 200, Vienna VA, 22182
NowSecure has 12 years in mobile app forensics, mobile app security testing, test automation, mobile pen testing and mobile security standards development.

Date Submitted: 6/16/21 Submitted by: Jeff Miller, Director US Public Sector - jmiller@nowsecure.com Gentry Sims, Director Fed Bus Dev - gsims@nowsecure.com	Contributors: Alan Snyder, CEO - asnyder@nowsecure.com Andrew Hoog, Founder - ahoog@nowsecure.com Brian Reed, CMO - breed@nowsecure.com Brendan Hann, PMM - bhann@nowsecure.com

0. NowSecure recommends elevating the effectiveness of binary analysis throughout the SBOM specification. It addresses many challenges highlighted in NTIA's request for comment. The advantages are listed here to simplify references to the benefits in our responses below. Binary analysis enables:

- a. Independent verification by testing without access to source code, guaranteeing the authenticity of the SBOM information
- b. Deeper assessments and identification of transitive dependencies (dependencies of dependencies) for greater coverage. For example, components in linked libraries like openssl and libpng will not be easily identified with source code analysis. These can help identify vulnerabilities and supply chain attacks.
- c. Immediacy by enabling testing of an executable/object code now while the industry implements the necessary tooling for complimentary source code analysis techniques.
- d. Automation for scale to cover millions apps already deployed in production and cover rapid update release cycles that can be daily.
- e. Ability to analyze a specific binary which is critical in threat hunting and identifying supply chain attacks.

The following responses map to the specific 'Request for Comment' items stated in NTIA's release document.
1. Are the elements described above, including data fields, operational considerations, and support for automation, sufficient? What other elements should be considered and why?

- a. Data Fields
  - i. Consider augmenting Supplier Name with optional Contact Information (e.g. email address) and/or Website URL. This could be pulled from publicly published component ecosystems (e.g. Maven, CocoaPods) to facilitate security communication, verification, etc.
  - ii. Cryptographic hash of the component can be difficult in many situations and maybe greatly reduce the signal-to-noise ratio. Consider making this optional/best effort and perhaps indicate how it was produced (examples include

    from component binary, as part of binary analysis of overall executable or perhaps as published by the component developer)
    - iii. Deep dependency relationships are critical to understanding the full SBOM and should be noted that simple Source Code Analysis will generally be unable to generate the SBOM of components (dependencies of dependencies). Emphasizing the benefits of binary analysis throughout the SBOM specification will greatly improve the impact of an SBOM.
- b. Operational considerations
    - i. Frequency should be updated for each new version of "supply chain software" (software used but not built by the recipient) which is not explicitly addressed. Binary analysis enables this for software used and can be automated to operate a scale.
    - ii. See 1(a)(iii) re: need to emphasize binary analysis. Binary analysis also enables the ability to use heuristics to identify what is known with confidence and to flag "coverage issues" (e.g. known unknowns). This approach (enumerating all references to components and looking for related metadata) creates a framework to not only measure completeness but also a measurement for uncertainty. Examples of uncertainty could include references to a component but no version information or references to a component yet no metadata about the component in available ecosystems.

2. Are there additional use cases that can further inform the elements of SBOM?
Based on the citation of unique characteristics below, we believe including mobile applications as on par with Software-as-a-Service is an important distinct addition to the specification.

- a. NowSecure recommends adding to use cases the analysis of “outbound service calls" as part of automated binary analysis for SBOM creation:
    - i. Automated dynamic binary analysis of apps run on real devices should assess outbound service calls to identify APIs and related functionality to identify where traffic is going, what data transmitted and validate accuracy of any previously created SBOM reports.
    - ii. Ensures the completeness of coverage through dynamic analysis that captures all real APIs accessed and information transmitted, while potentially uncovering attackers trying to obfuscate their data exfiltration through supply chain attacks.
- b. The other primary missing use case is for mobile apps which have grown dramatically in the past 10 years and now represent nearly 70% of all traffic on the Internet. The unique characteristics of this use case are as follows:
    - i. There are exponentially more mobile apps than traditional computer apps
    - ii. Mobile apps update at a significantly higher frequency (> 10 times a year, some weekly)
    - iii. Mobile devices operate both inside and outside traditional security barriers
    - iv. Mobile apps have access to vastly more invasive sensors that threaten privacy and access to sensitive data.
    - v. Mobile apps SBOMs can be generated via binary analysis at scale

3. SBOM creation and use touches on a number of related areas in IT management, cybersecurity, and public policy. We seek comment on how these issues described below should be considered in defining SBOM elements today and in the future.

- Issue “b” (Software-as-a-Service and online services) - See answer (2) above re: unique use case for mobile apps
- Issue “c” (Legacy and binary-only software) - See opening answer (0) re: binary analysis
- Issue “d” (Integrity and authenticity) - Integrity and authenticity: leveraging binary analysis can provide key verification of an SBOM which will add integrity to the results. In addition, digital signatures and PLI at scale are very difficult. However, with automated binary analysis, SBOM consumers can leverage a trusted vendor and access an SBOM over TLS which adds authenticity. The combination of these two techniques can accelerate the value of the impact of SBOMs quickly.
- Issue “e” (Threat model) - Binary analysis can target the specific executable/object code running on a system. As such, this technique is critical for the detection of internal compromise and advanced supply chain attacks.
- Issue “f” (High assurance use cases) - Binary analysis for mobile apps frequency surfaces compiler details (including anti-exploitation flags) as well as additional build data. Emphasizing the importance for this technique will add value to high assurance use cases.
- Issue “g” (Delivery) - See 3(d) above.
- Issue “h” (Depth) - See opening answer (0)(b) re: depth of analysis
    - i. While including identified vulnerability details in the SBOM is fine, it's critical that there's a process in place to reassess the components for newly discovered vulnerabilities. This requires automation to 1) scan all app updates, 2) ingest CVE and other vulnerability data, 3) re-analyze installed apps against new the new vulnerability data and 4) alert appropriate parties (e.g. the agency itself and the developer)

4. Flexibility of implementation and potential requirements. If there are legitimate reasons why the above elements might be difficult to adopt or use for certain technologies, industries, or communities, how might the goals and use cases described above be fulfilled through alternate means? What accommodations and alternate approaches can deliver benefits while allowing for flexibility?

- a. See opening answer (0)(c) re: the immediate value binary analysis can bring to the generation of SBOMs
- b. See opening answer (0)(d) re: how automated binary analysis can address the scale issue regarding the quantity of apps and their frequency of updates

NOTE: NowSecure has supporting evidence we can provide to this response. However, the data is proprietary and may be arranged for access, separate from the public response and engagement.