Section 4 Enhancing Software Supply Chain Security

4. Initial minimum requirements for testing software source code – EO Sections 4(e)(iv and v)

5. Guidelines for software integrity chains and provenance – EO Section 4(e)(vi)

Executive Order Section 4(e)(iv)

Every organization developing products which utilize third-party software components, either open-source or commercial-off-the-shelf, should have a standard operating procedure (SOP) integrated within their product lifecycle management function that details the steps required to detect and mitigate vulnerabilities.

Depending on the size of the organization, the SOP may span multiple functional groups or may be contained within a single functional group. In the former case, a typical, high-level workflow for such a procedure is shown in the following diagram:

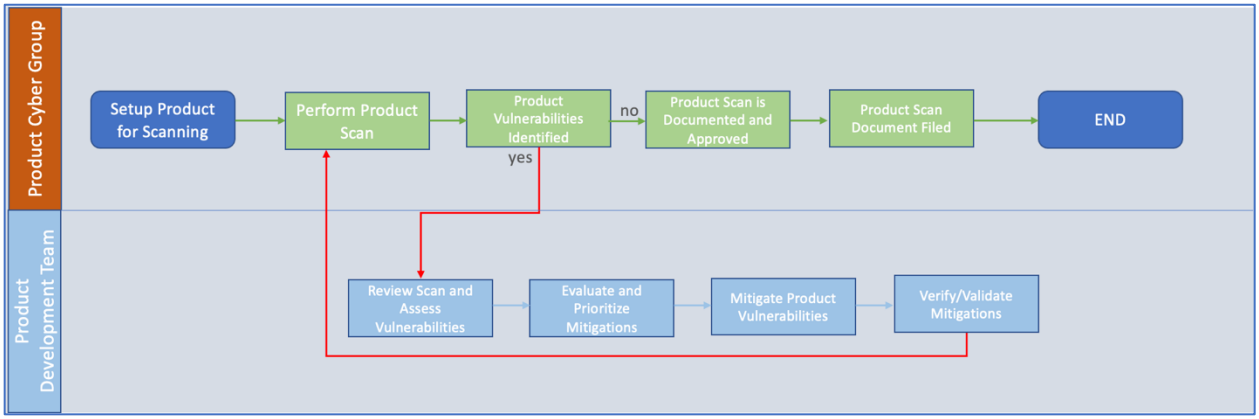

Figure 1. Product Vulnerability Scanning and Mitigation

Depending on various factors such as the complexity of the product, the automation level of the organization, and others, the timeline for the process in Figure 1 could span several days or weeks. The problem with this timeframe is that vulnerabilities are continuously surfacing, so without tools that help automate some of the process, organizations could find themselves falling further and further behind product launch schedules. This can result in products being shipped with known component vulnerabilities, as manufacturers move to meet demand or launch updates to existing products.

Executive Order Section 4(e)(v)

Providing the product purchaser artifacts of the above vulnerability scanning and mitigation process is a critical requirement in the enablement of product software transparency, however, the distribution of said artifacts must be controlled. "Public" distribution could prove dangerous, given that any useful artifact will likely contain security information easily leveraged by bad actors. Manufacturers will seek the least administratively burdensome distribution process, such as an authenticated portal site, however, purchasers will be seeking to minimize their time spent visiting portal sites, gathering security documentation. Available tools that provide cloud storage for upload and retrieval are another

option, but lacking a central location for all product security documentation, are still administratively burdensome. Eliminating this administrative burden, but controlling distribution, will ease adoption.

In terms of the information to include in the artifacts, including vulnerabilities and mitigations, as suggested in the Executive Order, will likely not be a viable option for newly launched products, but does make sense for existing, or legacy, products. If a newly launched product had vulnerabilities that were addressed prior to launch, there is not much benefit to be gained by the producer or consumer of that information, as it pertains to a pre-launch version of the product. For products that have already been launched into the marketplace, sometimes referred to as legacy products, showing that vulnerabilities were discovered and mitigated, could be helpful. For the producer, it will help communicate their security posture and ongoing lifecycle management of their products. For the consumer, it will provide confidence that security risks are being investigated and actions to mitigate are being taken. Again, controlled distribution of the artifacts, will be critical.

Executive Order Section 4(e)(vi)

In order to maintain accurate, up-to-date data about third-party software components, organizations will need to implement a process (see Figure 2) that begins with the generation of the product component list and enables eventual discovery of associated information about the software components, including vulnerability information.

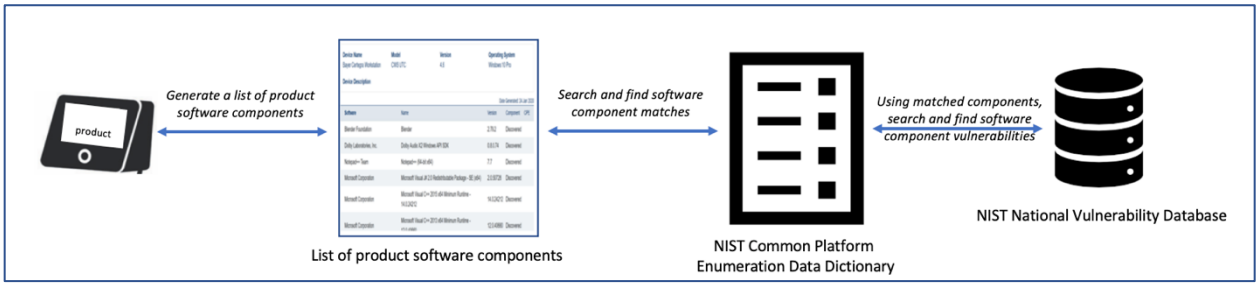

Figure 2. Maintaining Product Component Information Sample Process

This process involves generating a list of product software components, analogous to a list of ingredients in a food product. The importance of the software components is that each has its own security risk profile, and these aggregated component risk profiles, in turn, define the overall product risk profile. Using the list of product software components, producers can search publicly available data sources to find known vulnerabilities. Given the continuous evolution of vulnerabilities, this search and find process must also be executed continuously. Without accurate, current software component data, the product risk profile represents a static, and hence, inaccurate, measure of a product's associated risks.

Again, given the requirement for immediate reaction, the automation of some of the steps in the process shown in Figure 2 is of critical importance. Manual execution will cause delays in vulnerability discovery, causing opportunities for security breaches. In addition, accuracy of the publicly available information regarding third-party components will enable accurate reporting and artifacts, thus continuous maintenance of public data sources, such as those hosted by NIST, is critical.