DATE: May 26, 2021
COMMITTEE: NIST
ISSUE: Guidelines for software integrity chains and provenance
Author: Paul Russell, Chief Product Officer, Censinet, Inc., prussell@censinet.com

Supply Chain Transparency: Solution Bill of Materials

Our country's healthcare infrastructure is dependent on solutions composed of software, hardware, and people, often delivered and managed by private, third-party companies. While these solutions solve challenges the healthcare industry could not solve on its own, the solution components provide an increased attack surface area and a ripe environment for cyber threat actors.

First, most software depends on third-party components: libraries, executables, or source code. There is little-to-no visibility into this software supply chain which makes it challenging to know if the software used in any given organization contains an exploit. Second, hardware is built on a deep supply chain of components that are often developed in countries with a vested interest in infiltrating our country's infrastructure. Third, employees of third parties are frequently involved in the ongoing delivery of solutions. This can range from people managing revenue cycle activities to transcribing a doctor's audio recording of patient notes to the system administration and development of the software used in those activities. In all cases, effective organizational controls are as important as having incorporated the latest patched libraries in the software being used.

Most solution consumers are unable to enumerate the components that make up the solutions they use. Moreover, Censinet has found through its risk assessment platform that many third-party vendors do not notify their customers when there is a critical vulnerability in their solution. Relying on third parties to do the right thing requires not only the solution provider but all of the organizations supplying that provider to quickly and effectively communicate critical vulnerabilities. As a result, the current process for communicating vulnerabilities to solution consumers has numerous points of failure. It's little surprise that IBM's 2020 'Cost of a Data Breach Report' found that the average time to identify and contain a breach was 280 days.

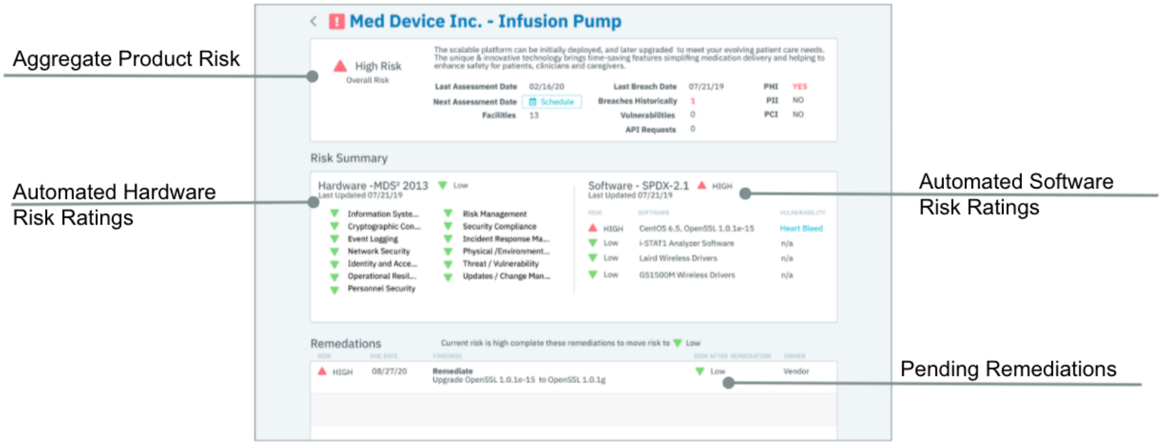
To ensure software integrity chains and provenance, we need to establish a model for communicating the components that make up not only the software, but also the hardware, people and processes that deliver solutions. With this level of transparency, solutions consumers can construct an inventory of all the components in use at their organization. When a component is discovered to have a vulnerability, an organization can easily identify that they have an issue in a downstream solution, and address it.

Call To Action

Censinet recommends establishing a working group to develop a standard for representing and communicating all constituent components making up any given solution (software, hardware, and associated human services). Ensuring that such an inventory is communicated, documented, and reviewed as a core part of standard risk assessments enables transparency into potential and actual vulnerabilities without relying on all parties in the supply chain to act and communicate effectively in a crisis.

The NTIA has established an ongoing Software Component Transparency effort to define a Software Bill of Materials (SBOM) definition. The NTIA SBOM website describes an SBOM as “a formal, machine-readable inventory of software components and dependencies, information about those components, and their hierarchical relationships.” The working group has made significant progress on developing a potential standard for communicating the components of any given software offering.

Expanding on the concept of a Software Bill of Materials and including the hardware components and organizational controls surrounding integrated human services provides a machine-readable way of communicating the inventory of components that constitute all aspects of a solution. This effectively creates a *Solution* Bill of Materials that brings transparency to both hardware and software components, their dependencies, and the human dependencies and controls implemented to manage their interaction.


Aggregate Product Risk
Automated Hardware Risk Ratings
Automated Software Risk Ratings
Pending Remediations

Med Device Inc. - Infusion Pump

▲ High Risk
Overall Risk

The scalable platform can be initially deployed, and later upgraded to meet your evolving patient care needs. The unique & innovative technology brings time-saving features simplifing medication delivery and helping to enhance safety for patients, clinicians and caregivers.

Last Assessment Date	02/16/20	Last Breach Date	07/21/19	PHI	YES
Next Assessment Date	Schedule	Breaches Historically	1	PII	NO
Facilities	13	Vulnerabilities	0	PCI	NO
		API Requests	0		

Risk Summary

Hardware -MDS² 2013 ▼ Low
Last Updated 07/21/19

- ▼ Information Syste...
- ▼ Cryptographic Con...
- ▼ Event Logging
- ▼ Network Security
- ▼ Identity and Acce...
- ▼ Operational Resil...
- ▼ Personnel Security
- ▼ Risk Management
- ▼ Security Compliance
- ▼ Incident Response Ma...
- ▼ Physical /Environment...
- ▼ Threat / Vulnerability
- ▼ Updates / Change Man...

Software - SPDX-2.1 ▲ HIGH
Last Updated 07/21/19

RISK	SOFTWARE	VULNERABILITY
▲ HIGH	CentOS 6.5, OpenSSL 1.0.1e-15	Heart Bleed
▼ Low	i-STAT1 Analyzer Software	n/a
▼ Low	Laird Wireless Drivers	n/a
▼ Low	GS1500M Wireless Drivers	n/a

Remedations

Current risk is high complete these remediations to move risk to ▼ Low

RISK	DUE DATE	FINDINGS	RISK AFTER REMEDIATION	OWNER
▲ HIGH	08/27/20	Remediate Upgrade OpenSSL 1.0.1e-15 to OpenSSL 1.0.1g	▼ Low	Vendor

Third-party risk assessments are a standard part of the solution acquisition process in healthcare. As they take place during the sales process, third parties are financially motivated to deliver required information and remediate issues that arise in order to close the sale. We can leverage the process and ongoing sales activities to drive transparency into the industry by requiring a *Solution* Bill of Materials during each risk assessment. This level of transparency enables solution consumers to programmatically generate a complete inventory of software, hardware, people, and process dependencies. Figure 1 shows a way to represent software component vulnerabilities in a medical device and calls attention to the use of a component vulnerable to the Heartbleed bug.

Using this approach, existing component vulnerabilities are easily identified during the risk assessment process. The ongoing management of vulnerabilities and gaps in third-party reporting is also mitigated by a *Solution* Bill of Materials. Risk management vendors can easily leverage the component data and known vulnerability databases to alert organizations using solutions with a newly discovered vulnerability.

Establishing a *Solution* Bill of Materials standard, required as part of a standard risk assessment, enables healthcare and other industries to drive ongoing improvement in third-party solution risk posture as well as rapid response to newly found vulnerabilities. We recommend establishing a working group with a mission to build on the NTIA SBOM paradigm to define a standard for the representation and exchange of the software, hardware, and human components and dependencies of solutions used in our critical infrastructure.