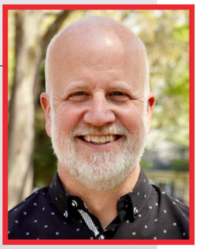
FEDInsider

How Government is Securing the Software Supply Chain

Government and industry are turning to SBOMs and stronger acquisition processes as the need to secure the software supply chain becomes more critical.

Featured Experts:

-
  Jason Mullins
  Supply Chain Lead,
  Department of Education
-
  Pat Sullivan
  Sr. Advisor to Director of Supply Chain Mgmt.,
  Army Material Command
-
  Justin Murphy
  Vulnerability Disclosure Analyst, CISA
-
  Robert Martin
  Sr. Principal Software & Supply Chain Assurance Engineer, MITRE
- 
  Sam Kinch
  Director, Technical Acct. Management-Federal,
  Tanium

Cyberattacks are only getting more sophisticated, especially with a tactic called the "bank shot." This refers to planting malicious code in software components before they're used in products, so coders unknowingly include the malware when drawing on software libraries. This poses a new risk to the software supply chain and systems capable of patching themselves — and automatic patching is critical to protecting legacy systems.

With attacks becoming more complex, the National Security Agency and the Cybersecurity and Infrastructure Security Agency has released new guidance, "Securing the Software Supply Chain: Recommended Practices Guide for Customers," to provide steps that agencies should take to ensure the integrity of the software they buy. Members of government and industry recently spoke at a FedInsider panel to discuss how they are using SBOMs to identify, manage and mitigate these new cybersecurity risks.

STATE OF SOFTWARE SUPPLY CHAIN SECURITY

Software is comprised of several different components and frameworks, assembled to create the capabilities and specifics of an application.

"Government agencies are going to have a large software supply chain," said Jason Mullins, supply chain lead with the U.S. Department of Education. Considering software supply chains start with acquisition, Mullins said it's important to understand who made the component, and what it's made of.

That starts with visibility. Justin Murphy, a vulnerability disclosure analyst with the Cybersecurity Infrastructure Security Agency, said when Apache Log4j was experiencing a software vulnerability — a software widely used in websites, applications and operational technology — organizations needed to figure out quickly where Log4j was in their products.

"It turned out it can be a whole bunch of different places," Murphy said, "and without having greater visibility into the supply chain of our products, servers and operational technology and all of our software we have custom developed to do cool things to make the world a better place... it was difficult to know what was in our software and what we had to address."

And while not all vulnerabilities are going to put an organization at risk, having that visibility will help IT teams know whether a software vulnerability is contained in the software or exploitable to the rest of the supply chain. That's something CISA is working on.

The Army Materiel Command (AMC), on one hand, has over 2,000 supply chain managers monitoring its supply chain from end-to-end, starting with validated demand for capability through the acquisition process, all the way through the decision and distribution cycle. Then, it's managed across the entirety of the software lifecycle.

"We have a process that talks about pre-cradle-to-grave. And in the software supply chain there is nuanced differences with both how the supply chain works and how we monitor it in the end," said Pat Sullivan, senior advisor to director of supply chain management with AMC.

The increasing use of pre-build code libraries, which are available to developers, also demonstrates the critical nature of a cybersecurity program designed for the software supply chain, according to Sam Kinch, director of the technical account management with Tanium Federal.

And that program can't be static or unique to a single code. "It has to be something that is ongoing throughout the use of the software... real-time knowledge of your software and software dependencies your company utilizes really is the first step in defending it," Kinch said.

RESPONDING TO TODAY'S SOFTWARE SUPPLY CHAIN CRITICALITY WITH SBOMS

Organizations are increasingly reusing components of software to build out their own products. "Getting attestations about how the software was created, tested, maybe where it came from, maybe who was involved, all of that has really come together, and I think it is time," said Bob Martin, senior principal software and supply chain assurance engineer with MITRE.

That's where Software Bill of Materials, or SBOMs, come in. A mandate in 2021 requires software developers who do business with the federal government to include an "ingredient list" with a software package detailing the software components and what the developer used. SBOMs will also require updates as software components evolve.

And creating SBOMs also starts with visibility, Mullins said. "You need to know all the environments and all the different places it resides, and you have to perform assessment and continuous monitoring," he said.

SBOMs allow for a more granular approach to visibility and continuous monitoring. Agencies can build a provenance database and repository of SBOMs to anticipate the next Log4j, instead of having to do all the groundwork when the next Log4j happens. This way, IT leaders can easily see where the software is affected. "So when this bit of software that is connected to the system is affected, I start acting on that in an actionable way," Mullins said.

For the AMC, Sullivan said SBOMs provide a complement to the data that enables other processes like instant response and continuous monitoring. "It is a valuable tool to help not only at the point of crisis, but as we work every day to detect and deny identified and malicious intent," he said. And soon, the Army will be diving "headfirst" into SBOMs.

Even when not in a crisis, if SBOMs are used for everything on every device in an enterprise, agencies will have much finer detail of what's going on in their enterprise. "That will inform your discussions from continuous monitoring or vulnerability management. Or if you're doing threat intelligence, you look at what you are seeing there and compare it to your environment and your susceptibility," Martin said.

MOVING FORWARD WITH SBOMS

Kinch added, because SBOMs can't be static, Tanium has a feature that can analyze software to give customers a continuous real-time SBOM so that if there's a new vulnerability, they immediately know the extent of the threat and its location. "This process is significantly reducing the vulnerability window that a company will experience when an exploit is released," said Kinch.

According to Murphy, the government still has some kinks to work through since all vendors who want to sell to the U.S. government must provide an SBOM, and — with the massive amount of software the government purchases — this could create a data management challenge, which is something CISA is working through. "We need to work on the consumption side of things regarding the maturity of the generation of tools at CISA," he added.

And while government and industry work together to mature software supply chain security through solutions like SBOMs, ultimately, it must be a holistic approach — starting with the acquisition process.

Hosky Communications Inc.
3811 Massachusetts Avenue, NW
Washington, DC 20016
Contact: **John Hosky**

☎ (202) 237-0300
✉ Info@FedInsider.com
🌐 www.FedInsider.com
f @FedInsiderNews
in Linkedin.com/company/FedInsider
t @FedInsider

Carahsoft
1493 Sunset Hills Road
Reston, VA 20190
Contact: **First Last**

☎ (703) 230-7597
✉ Tanium@Carahsoft.com
🌐 www.Carahsoft.com/Tanium
f Facebook.com/Carahsoft
in Linkedin.com/company/Carahsoft
t @Carahsoft

Tanium
6700 Rockledge Drive, Suite 540A
Bethesda, MD 20817
Contact: **First Last**

☎ (510) 704-0202
✉ Tanium@Carahsoft.com
🌐 www.Tanium.com
f Facebook.com/Tanium
in Linkedin.com/company/Tanium
t @Tanium