What Government Can Learn About Supply Chain Security From SolarWinds Breach

Leaders look to newer focuses in securing their ICT supply chains.

Kate Macri
Fri, 12/18/2020 - 16:07

The Cybersecurity and Infrastructure Security Agency's guidelines on information and communications technology (ICT) supply chain risk management (SCRM) are necessary to preventing such breaches like the one seen last week.
On the heels of FireEye’s discovery of a SolarWinds software supply chain breach, which cascaded into a cyberattack exposing multiple federal agencies, government contractors and state governments, the Government Accountability Office identified most federal civilian agencies are not implementing ICT SCRM practices according to CISA's guidelines.

“The practice with the highest rate of implementation was implemented by only six agencies,” GAO said in its Dec. 15 report. “Without establishing executive oversight of SCRM activities, agencies are limited in their ability to make risk decisions across the organization about how to most effectively secure their ICT product and service supply chains. Moreover, agencies lack the ability to understand and manage risk and reduce the likelihood that adverse events will occur without reasonable visibility and traceability into supply chains.”

Federal software supply chain threats are expected to intensify. In September 2019, CISA said federal agencies faced at least 180 different kinds of ICT supply chain threats, and CISA's November 2020 report highlighted how an overreliance on single-source suppliers is a high-priority risk for ICT supply chains. Widespread use of and reliance on SolarWinds software, for example, resulted in a cyberattack of unprecedented scale and scope across the .gov landscape as well as their private-sector vendors.

The growing use of commercial, off-the-shelf software and open-source-based software applications for federal use also pose risk to federal agencies, according to Daniel Kroese, associate director of CISA’s National Risk Management Center.

“Software represents a potentially concentrated source of risk if you don't have the vulnerability management and acquisition strategies around it,” Kroese said during an ICT supply chain security panel at a GovernmentCIO Media & Research event in October. “We're working to deploy a series of tools across government agencies, but also private-sector partners in the critical infrastructure community to do this supply chain analysis so that if there are vulnerabilities ... we can track it, understand where it is and patch that swiftly.”

A simple software update could hide malware, according to Atlantic Council cyber expert Trey Herr in a July report.

FireEye confirmed the SolarWinds hack began with a tainted software update “in order to distribute malware we call SUNBURST,” according to the cybersecurity firm’s
technical report on the attack.

“They gained access to victims via trojanized updates to SolarWind’s Orion IT monitoring and management software,” FireEye said. “This campaign may have begun as early as Spring 2020 and is currently ongoing. Post compromise activity following this supply chain compromise has included lateral movement and data theft.”

According to GAO's report, only four civilian federal agencies deployed an agency-wide SCRM strategy, but did not account for risks associated with the software development lifecycle, like software updates.

GAO’s report also predicted foreign actors would increasingly target ICT supply chains.

“Supply chains are being targeted by increasingly sophisticated and well-funded threat actors including leading foreign cyber threat nations such as Russia, China, Iran and North Korea,” GAO said in its report. “Attacks by such entities are often especially sophisticated and difficult to detect. In addition, threat actors attack all tiers of the supply chain and at each phase of the system development life cycle and, thus, pose significant risk to federal agencies.”

In a footnote, GAO listed “software development environments” as a potential supply chain target for foreign actors.

The report also details that the civilian federal agencies listed were planning to deploy the SCRM best practices by the end of fiscal year 2020.

CISA continues to spearhead the defense of federal ICT supply chains. CISA’s ICT SCRM Task Force just released a report highlighting the task force’s progress “to advance meaningful partnerships and analysis around supply chain security and resilience” in its first two years.

The Task Force, which includes the Department of Homeland Security, the Office of the National Director of Intelligence, the Nuclear Regulatory Commission and private sector IT vendors, emphasized information-sharing and supply chain mapping, and also developed a template for SCRM compliance assessments. These template assessments include reviews of software integrity.
“Supply chain security is a matter of urgency and consequence, and the best way to increase our defenses is through substantial coordination and cooperation between government and industry,” said Robert Mayer, co-chair of the ICT SCRM Task Force. “This is a partnership that will expand in 2021 and further strengthen the security and resiliency of our supply chain.”

As CISA, the FBI and ODNI lead the SolarWinds hack response, CISA continues drilling down on ICT SCRM best practices and providing a wealth of guidance and assistance for federal agencies and their vendors via the National Risk Management Center.

As Kroese said at the GovernmentCIO Media & Research event in October, software integrity is more important than ever for cybersecurity professionals at federal agencies.

“Before you would have physical switches and lines in the ground, and now a whole host of functionality is now controlled by software when before it was the physical arrangement,” he said. “You have the software that enables the firmware capabilities. What if those monthly software updates introduce more vulnerability to the system? It's really hard to differentiate the line between where the software ends and the hardware starts.”

View printer friendly version
Federal Cybersecurity
CISA
GAO
Department of Homeland Security
FBI
ODNI
SolarWinds
FireEye
ICT supply chain
software
Standard