NISOS
Webinar Brief

The SolarWinds Breach: Where Do We Stand One Year Later?

Main Takeaway

As a result of the SolarWinds breach and Log4J vulnerability, we are likely to see a major regulatory environment shift from static third-party vendor questionnaires to dynamic, modularized, automated, monitoring processes that provide insight into supply chain vulnerabilities.

Executive Summary

The SolarWinds breach of December 2020 was an unprecedented supply chain attack by the Russian SVR against 18,000+ customers of the network monitoring vendor, SolarWinds. The threat actors were able to embed malicious code in the SolarWinds Orion product. Every time one of the 18,000 customers updated Orion, Russian actors were able to gain backdoor access to the victim's environment.

Additional Supply Chain Attacks

The Log4J vulnerability enabled remote code execution against servers using the Java-based logging utility within the Apache Logging Service. These attacks have a major impact as all applications in modern-day enterprises a) run a compilation and variety of open-source libraries that could be vulnerable to the same attack, and b) have a defined process that submits code to production updates.

These supply chain attacks disrupt a security team's ability to discern what is truthful, accurate, and complete within their applications. Unlike traditional attacks like phishing emails, these attack directly establish footholds via software backdoors.

Vendor Assessments More Scrutinized

SolarWinds and Log4J have raised awareness of supply chain vulnerabilities in the SDLC. Both attacks raise awareness of the far-reaching implications of attackers exploiting the build process of SDLC and highlight the prevalence of Orion and Log4J in almost all of the world's software applications. Exploiting these applications allowed attackers to access sensitive environments at a previously unrealized scale.

As a result, open-source software, software bill of materials (SBOMs), dependencies, and libraries are now being inspected more closely by enterprise security teams and contractual agreements and vendor governance requirements are receiving greater scrutiny.

Remediating vulnerabilities like Log4J is relatively straight-forward in SaaS environments where updates can be quickly deployed, but if the vulnerable software resides on customer laptops and releases happen infrequently, the risk increases. Conducting attack surface management and using threat intelligence to understand how many vulnerable libraries exist in enterprise software is a good first step to identify and patch vulnerable systems.

Overhaul is Needed in Software Development Life Cycle

Technology development is largely unregulated and developers often write large amounts of code on top of one another in CICD or Agile environments. According to our experts, eighty percent (80%) of written code is either open-source or another developer's code. The remaining twenty percent (20%) is custom written for a particular function. While large enterprises regularly vette software through the contracting process, they typically do not vette libraries and dependencies for security concerns. However, we predict more regulation will be initiated due to the criticality of the software build process and its potential impact on the technology supply chain. Mandating the use of SBOMs to help increase transparency around the provenance of software is one viable approach.

Third-Party Supply Chain Risk Must Become Dynamic; Not Point-in-Time

We are likely to see a major regulatory shift from point-in-time third-party vendor questionnaires to an ongoing and automated monitoring process. Options are emerging that not only identify vulnerabilities, but also use external telemetry to determine if these

vulnerabilities have been exploited. A robust attack surface monitoring program can enhance routine vulnerability management for critical third-party libraries and other supply chain efforts. These programs can be built in-house or can be run by outside experts.

For more information on how to build such a program or vette your supply chain, contact the experts at Nisos.

About Nisos

Nisos is the Managed Intelligence Company™. Our services enable security, intelligence, and trust & safety teams to leverage a world-class intelligence capability tailored to their needs. We fuse robust data collection with a deep understanding of the adversarial mindset delivering smarter defense and more effective response against advanced cyber attacks, disinformation and abuse of digital platforms. For more information visit: **www.nisos.com**

This briefing is not legal advice and is provided for general informational purposes only.