REVERSINGLABS

Why Software Supply Chain Security Matters to Development Teams

742%

increase in software supply chain attacks²

Up to



of application code can be open source that is vulnerable to attack³

Millions \$\$

in damages & lost shareholder value caused by software supply chain attacks⁵ Historically, unpatched vulnerabilities were targeted and exploited when executing software supply chain attacks. However, according to CISA, the nature of these attacks has changed. Recently, threat actors have been injecting malicious code into open source and software products which enterprises download and integrate into their systems, exposing them to malware¹.

These types of attacks are increasingly common, with software supply chain attacks rising by 742%². This increase is due to a greater dependence on open source packages with up to 90% of code in applications being open source³, as well as outdated tooling and security practices, leaving enterprises vulnerable to new attack vectors.

In fact, Lapsus\$, a data extortion group, organized a supply chain attack when they accessed Okta's administrative accounts and embedded malicious code into their identity management platform. When 366 users updated their platform, malware entered their environment⁴. This caused millions of dollars in damages and Okta's share price to drop 11% over the following week⁵.

To prevent similar attacks, it is essential to validate the integrity of code for open source and third party software components by identifying undocumented features, suppliers' change of location or ownership, and abnormal timing and frequency of updates. This helps developers secure builds, software development, and their attack surface⁶.

Traditionally, teams use software composition analysis (SCA) tools to protect themselves from supply chain attacks; however, they exclusively detect vulnerabilities in open source components. Their legacy approach provides inadequate coverage for newer practices where attackers insert malicious code into open source and software components. This is because they fail to monitor 3rd party software updates, cannot identify active threats or tampering in codebases, and cannot locate the suspicious behaviors listed above.

The tactics, techniques, and procedures (TTPs) for supply chain attacks are quickly evolving, and enterprises and their tools are struggling to adapt, leaving them at risk for supply chain incidents.

How Developers Can Prevent Software Supply Chain Attacks

Establishing secure and repeatable software development practices enables developers to identify and respond to severe threats, which NIST's secure software development framework (SSDF) enforces.

NIST developed the SSDF to ensure that "all software components are protected from tampering and unauthorized access, well-secured software with minimal security vulnerabilities is released, and vulnerabilities are identified and properly addressed while similar ones are prevented from occurring in the future" ⁷.

Sources:

- ¹ https://www.cisa.gov/sites/default/files/publications/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN_DEVELOPERS.PDF
- ² https://scribesecurity.com/software-supply-chain-security/supply-chain-risks/#the-known-vulnerabilities-in-software-supply-chains
- ³ https://techcrunch.com/2019/01/12/how-open-source-software-took-over-the-world
- ⁴ https://www.thirdpartytrust.com/blog/okta-breach-preventing-supply-chain-attacks
- ⁵ https://www.reuters.com/technology/okta-says-up-366-customers-have-potentially-been-impacted-by-hacker-attack-2022-03-23
- ⁶ https://www.cisa.gov/sites/default/files/publications/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN_DEVELOPERS.PDF
- ⁷ https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf

Protect software

 Protect all forms of code from unauthorized access or tampering

• Provide a mechanism for verifying software release integrity

• Archive and protect each software release

Produce secure software

• Verify that 3rd party vendors align with internal security practices

• Configure the build process to eliminate vulnerabilities before testing

• Test executable and human-readable code

Respond to vulnerabilities

 Identify and confirm vulnerabilities on an ongoing basis

 Assess, prioritize, and remediate code-based vulnerabilities

• Analyze vulnerabilities to identify their root causes

The SSDF helps development teams produce secure builds, release safe code, secure their systems from future attacks, and protect against new TTPs for software supply chain attacks. It recommends that teams achieve 3 things: Protect software, produce secure software, and respond to vulnerabilities. Listed above are their critical practices for enforcing each guideline⁸.

The SSDF ensures that development teams effectively create secure software and maintain its integrity. By verifying releases, protecting code from tampering, and monitoring third party softwares and updates, enterprises can see where code is located and how it has been changed, helping discover software supply chain attacks in pre-production.

How ReversingLabs addresses the SSDF and protects against software supply chain attacks

SAST, DAST, and SCA tools follow parts of the "produce secure software" and "respond to vulnerabilities" sections of the SSDF by continuously scanning for common vulnerability exploits (CVEs), providing alerts with context, and testing source code. This helps teams quickly identify and remediate vulnerabilities and review code. However, they do not address the critical "protect software" section which ensures that active threats like malware and tampering are identified in components and code in pre-production. With supply chain attackers embedding malicious code in components, users are at risk for these incidents.

The ReversingLabs Software Supply Chain Security (SSCS) Platform provides critical coverage and follows each section of the SSDF. It does this by identifying active threats like malware and tampering, validating the integrity of open source and product updates, supplying contextual alerts, and scanning for CVEs. This helps enterprises validate the integrity of their builds, code embedded in open source and third party software components, and identify and quickly remediate vulnerabilities, protecting them from software supply chain incidents, establishing effective security practices, and achieving SSDF compliance.

The ReversingLabs SSCS platform secures open source and 3rd party software components and protects organizations from persistent and major threats and risks. With a holistic approach to supply chain security, our platform enables enterprises to effectively identify and respond to threats, develop effective security practices, and achieve compliance.

Compliance

Achieve NIST SSDF, ISO and FFIEC supply chain, and HITRUST 3rd party risk management compliance.

Comprehensive Security Coverage

Monitor and secure open source and 3rd party software components to identify malicious updates and packages.

Active Threat Detection

Identify and eliminate malware and tampering before deployment.

Contextual Alerting

Ranks alerts by severity and time to resolve to help teams efficiently respond to the right threats and vulnerabilities.

Risk Auditing

Collect a software bill of materials (SBOM) and historical record to identify all 3rd party software and open source components that existed in your environment to visualize your attack surface.

Suspicious Behavior Identification

Understand baseline behaviors and identify suspicious actions and anomalies.

Policy Customization

Create custom policies to locate and prioritize threats and risks specific to your environment and enforce consistent security standards.

Get Started!

REQUEST A DEMO

www.reversinglabs.com

About ReversingLabs

ReversingLabs, the leader in software supply chain security, offers the only holistic software supply chain solution that secures 3rd party software and open source components and identifies active threats. ReversingLabs provides protection against malware and tampering in pre and active production. For more information or to schedule a demo, contact us today.



© Copyright 2023 ReversingLabs. All rights reserved. ReversingLabs is the registered trademark of ReversingLabs US Inc. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

Worldwide Sales : +1.617.250.7518 sales@reversinglabs.com