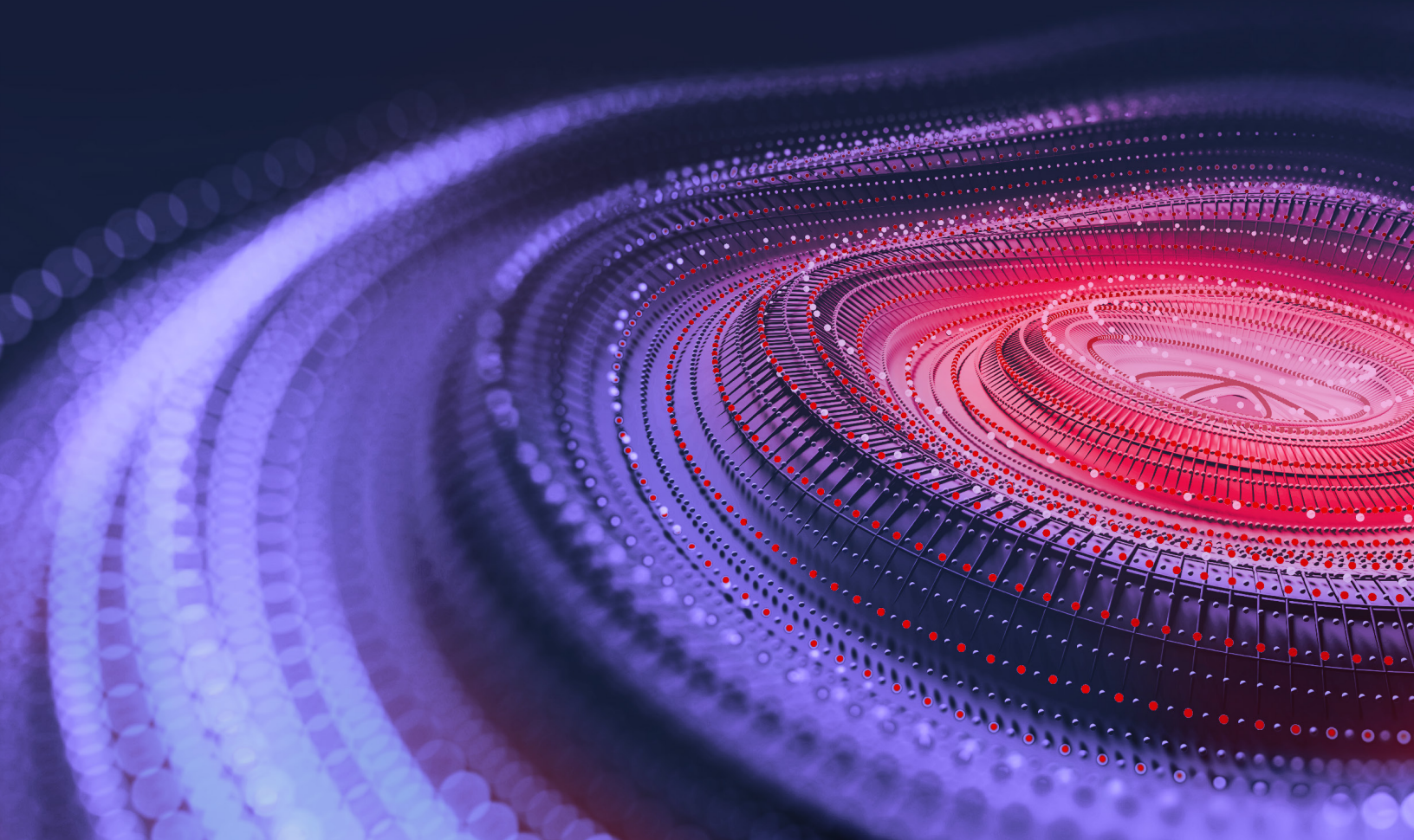
SOLUTION BRIEF

REVERSINGLABS

Why Software Supply Chain Security Matters to Software Producers



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 malware[1].

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to a greater dependence on open-source packages with up to 90% of code in applications being open source[3], as well as outdated tooling and security practices, leaving enterprises vulnerable to new attack vectors.

742%

increase in software supply chain attacks [2]

Up to

90%

of application code can be open source that is vulnerable to attack [3]

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 environment[4]. This caused millions of dollars in damages and Okta's share price to drop 11% over the following week[5].

Mill. $$

in damages & lost shareholder value caused by software supply chain attacks [5]

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 producers secure builds, software development, and their attack surface[6].

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 third-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 Producers Can Prevent Software Supply Chain Attacks

Establishing secure and repeatable software development practices enables producers 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].

Protect Software	Produce Secure Software	Respond to Vulnerabilities
• Protect all forms of code from unauthorized access or tampering • Provide a mechanism for verifying software release integrity • Archive and protect each software release	• Verify that third-party vendors align with internal security practices • Configure the build process to eliminate vulnerabilities before testing • Test executable and human-readable code	• 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 guideline[8].

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 Spectra Assure 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.

Spectra Assure Features

Spectra Assure secures open source and third-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 third-party risk management compliance.

Contextual Alerting

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

Suspicious Behavior Identification

Understand baseline behaviors and identify suspicious actions and anomalies.

Comprehensive Security Coverage

Monitor and secure open source and third-party software components to identify malicious updates and packages.

Risk Auditing

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

Policy Customization

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

Active Threat Detection

Identify and eliminate malware and tampering before deployment.

Learn More about ReversingLabs

ReversingLabs is the trusted authority in file and application security, protecting software development and powering advanced security solutions for the most advanced cybersecurity and Fortune 500 companies. The ReversingLabs Titanium Platform® powers the software supply chain security and threat intelligence solutions essential to advancing enterprise cybersecurity maturity globally. Tracking over 35 billion files daily, and the ability to deconstruct full software binaries in seconds or minutes, only ReversingLabs provides that final exam to determine whether a single file or full software binary presents a risk.

Get Started!

We'll Show You How To Reduce Software Supply Chain Risks With ReversingLabs

REQUEST A DEMO

www.reversinglabs.com

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
[8] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf

REVERSINGLABS

Worldwide Sales: +1.617.250.7518
sales@reversinglabs.com