Rezilion

6 Examples of Software Supply Chain Attacks (And How to Prevent Them)

SOFTWARE SUPPLY CHAIN ATTACKS TARGET ORGANIZATIONS by going after their third-party vendors or suppliers of software, hardware, or services at any stage of the development lifecycle. The goal is to gain access, conduct espionage, and enable sabotage.

These attacks range from using simple deception techniques such as disguising malware as legitimate products to more complex means to access and modify a legitimate program's source code. Besides compromising the infrastructure of developers and distributors, adversaries may try to exploit tools, dependencies, shared libraries, and third-party code.

SolarWinds is perhaps still the most well known of software supply chain attack victims. But here is a look at six others.

! KASEYA

Kaseya, an IT management company, announced in July 2021 that its VSA software had been exploited and 60 customers and another 1,500 businesses were impacted.

! CODECOV

Prior to the Kaseya attack, in April 2021, software testing platform Codecov, which generates code coverage reports and statistics, discovered it was targeted by a supply chain attack that manipulated Docker upload scripts.

! OKTA

In 2022, Okta, a provider of authentication services with more than 15,000 global clients, disclosed three breaches that year — the most recent of which was the compromise of its GitHub repositories.

! THE GITHUB OAUTH TOKENS ATTACK

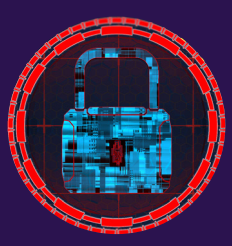
In April 2022, repository hosting service GitHub revealed that an attacker had stolen OAuth user tokens issued to third-party integrators Heroku and Travis-CI, which were used to download data from dozens of GitHub's customers.

! THE FISHPIG MAGENTO HACK

UK-based e-commerce software maker FishPig, discovered a security breach of its distribution server that gave threat actors the ability to control its systems and infect customers of its fee-based Magento 2 open source WordPress modules. The supply chain attack took place in August 2022.

! LOG4J

Log4j reveals more of a massive "potential" for attack, but is a significant example of the inherent vulnerability in the software supply chain. At the end of 2021, a Java-based logging utility known as Log4j fell victim to a vulnerability, Log4Shell, and put millions of computers at risk. Log4j is open source software that was built by the Apache Software Foundation to record diagnostic information about systems.



How to Protect Yourself From Software Supply Chain Attacks

It is difficult to prevent software security attacks because of the vast number of suppliers in the supply chain. But there are some rules of thumb to follow:

- ✓ **Keep an updated inventory of all your software assets with a Software Bill of Materials (SBOM)**
- ✓ **Secure your endpoints**
- ✓ **Implement solid code integrity policies that include stringent rules to authorize apps**
- ✓ **Prepare an incident response plan to protect all mission-critical components**

How Rezilion Can Help You Defend Against Software Supply Chain Attacks

TRUE DEFENSE OF THE SOFTWARE ATTACK SURFACE REQUIRES A DYNAMIC SBOM. A Dynamic SBOM creates a continuous inventory of all of your software components, maps any recognized vulnerability to these components, and assesses your attack surface. Learn more about how we can help you create a Dynamic SBOM at www.rezilion.com/platform/sca-dynamic-sbom/.