Top 10 CI/CD Security Risks

By Authors

CI/CD environments, processes, and systems are the beating heart of any modern software organization. They deliver code from an engineer's workstation to production. Combined with the rise of the DevOps discipline and microservice architectures, CI/CD systems and processes have reshaped the engineering ecosystem:

- The technical stack is more diverse.
- Adoption of new languages and frameworks is increasingly quicker.
- There is an increased use of automation and Infrastructure as Code (IaC) practices.
- 3rd parties (dependencies and services) have become a major part of any CI/CD ecosystem, with the integration of a new service typically requiring no more than adding 1-2 lines of code.

These characteristics allow faster, more flexible and diverse software delivery. However, they have also reshaped the attack surface with a multitude of new avenues and opportunities for attackers.

Adversaries of all levels of sophistication are shifting their attention to CI/CD, realizing CI/CD services provide an efficient path to reaching an organization's crown jewels. The industry is witnessing a significant rise in the amount, frequency and magnitude of incidents and attack vectors focusing on abusing flaws in the CI/CD ecosystem, including –

- The compromise of the **SolarWinds** build system
- The **Codecov** breach
- The **PHP breach**
- The **Dependency Confusion** flaw
- The compromises of the ***ua-parser-js, coa*** **and** ***rc*** **NPM packages**

While attackers have adapted their techniques to the new realities of CI/CD, most defenders are still early on in their efforts to find the right ways to detect, understand, and manage the risks associated with these environments.

This document helps defenders identify focus areas for securing their CI/CD ecosystem. It is the result of extensive research into attack vectors associated with CI/CD, and the analysis of high profile breaches and security flaws.

Numerous industry experts across multiple verticals and disciplines came together to collaborate on this document to ensure its relevance to today's threat landscape, risk surface, and the challenges that defenders face in dealing with these risks.

The list was compiled on the basis of extensive research and analysis based on the following sources:

- Analysis of the architecture, design and security posture of hundreds of CI/CD environments across multiple verticals and industries.

- Profound discussions with industry experts.
- Publications detailing incidents and security flaws within the CI/CD security domain.
