Learn: CI/CD and Supply Chain Security

How build pipelines, source control, and package registries get turned into an attack path. Pipelines run untrusted code with powerful credentials, so one poisoned build can reach production.

HOW IT WORKS

01 Topics

How build pipelines, source control, and package registries get turned into an attack path. Pipelines run untrusted code with powerful credentials, so one poisoned build can reach production.

- What is CI/CD Pipeline Poisoning?: Get attacker-controlled code to run in a privileged build. A malicious commit, pull reques
- What is Pull Request Injection?: Open a malicious pull request whose code or CI config runs when the PR is built. On pipeli
- What is a Package Registry Attack?: Builds install dependencies automatically. An attacker abuses the registry or its proxy, t

SOURCES

[1] OWASP Top 10 CI/CD Security Risks

Find the CI/CD and supply-chain risks before an attacker does.

securelayer7.net/learn/ci-cd-security

Open online