What is CI/CD pipeline poisoning?

CI/CD pipeline poisoning is abusing a continuous-integration pipeline to run attacker-controlled code in a privileged build environment. A malicious commit, pull request, or dependency triggers the pipeline, which then exposes runner secrets, cloud credentials, and deploy keys, or ships tampered artifacts to production. Because pipelines are trusted and hold powerful credentials, one poisoned build can reach production. Defend by isolating untrusted builds, least-privilege runners, and reviewing pipeline changes.

HOW IT WORKS

01 How it works and example

The attacker introduces code or a build-config change that the pipeline runs, then uses that execution to dump runner environment variables, read cloud credentials, sign or publish tampered artifacts, or reach internal systems the runner can touch. In a 2026 intrusion, a malicious pull request was opened specifically to trigger credential probing in the runner environment.

SOURCES

[1] OWASP Top 10 CI/CD Security Risks

[2] HuggingFace, Agent intrusion technical timeline

[3] MITRE ATT&CK: Supply Chain Compromise (T1195)

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

securelayer7.net/learn/ci-cd-security/ci-cd-pipeline-poisoning

Open online