What is a package registry attack?

A package registry attack abuses the systems that host and proxy software dependencies to get malicious or unexpected code into a build. Techniques include typosquatting, dependency confusion, and exploiting a proxy cache or registry itself, sometimes to gain egress from an otherwise isolated build environment. Because builds install dependencies automatically, a poisoned package runs with the build's privileges. Defend by pinning and verifying dependencies, using a private registry with an allowlist, and isolating build egress.

HOW IT WORKS

01 How it works and example

Common techniques are typosquatting a popular package name, dependency confusion where a public package shadows an internal one, and exploiting the registry or proxy cache directly. In a 2026 intrusion, a zero-day in a package proxy cache was used to gain internet egress from an otherwise isolated evaluation environment, turning dependency resolution into a foothold.

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/package-registry-attack

Open online