

OWASP CI/CD Security Risks and Real-World Examples

1. Insecure Secrets Management

Example: In 2021, Uber's private repositories were breached when an attacker accessed hardcoded credentials in a CI/CD pipeline. This led to unauthorized access to internal systems.

2. Poisoned Pipeline Execution (PPE)

Example: The Codecov breach in 2021 involved attackers injecting malicious code into a CI/CD script, allowing them to steal credentials and source code from multiple organizations.

3. Dependency Chain Attacks

Example: The 2020 SolarWinds attack compromised the CI/CD pipeline by injecting a backdoor into software updates, affecting thousands of organizations, including government agencies.

CI/CD Security Checklist:

1. Secure Secrets: Store credentials in a vault and avoid hardcoding secrets in repositories.
2. Pipeline Integrity: Use code signing and enforce strict access controls.
3. Third-Party Security: Audit dependencies regularly and use Software Bill of Materials (SBOM) tools.
4. Environment Segmentation: Keep build, test, and deployment environments separate.
5. Automated Security Scans: Use static and dynamic analysis tools to detect vulnerabilities.
6. Access Controls: Restrict CI/CD pipeline access by roles and enforce multi-factor authentication (MFA).
7. Monitoring & Logging: Enable real-time monitoring to detect unauthorized access.
8. Reproducible Builds: Ensure builds match source code for integrity.
9. Supply Chain Security: Verify third-party tools, libraries, and containers.
10. Incident Response Plan: Develop and test a plan to address security breaches.

Following these practices helps secure CI/CD pipelines against real-world threats.