
AWS
re:Invent
DECEMBER 2 – 6, 2024 | LAS VEGAS, NV

SEC339

Mitigating OWASP Top 10 CI/CD security risks using AWS services

Daniel Begimher
Senior Security Engineer
Global Services Security
AWS

Patrick Gaw
Senior Manager Security Engineering
Global Services Security
AWS

Purpose and agenda

Purpose

Learn how to mitigate security risks against your CI/CD pipelines

Agenda

- Background
- OWASP Top 10 CI/CD risks
- Challenge
- Whiteboarding
- Session summary

Background

500+

Average number of open source components[1]

96%

Percentage of software containing open source[1]

59%

Percentage of survey respondents affected by software supply chain attacks[2]

1 Synopsys, 2024; 2 Ponemon Institute, May 2024

OWASP Top 10 CI/CD security risks

CICD-SEC-1

Insufficient Flow Control Mechanisms

CICD-SEC-2

Inadequate Identity and Access Management

CICD-SEC-3

Dependency Chain Abuse

CICD-SEC-4

Poisoned Pipeline Execution (PPE)

CICD-SEC-5

Insufficient PBAC (Pipeline-Based Access Controls)

CICD-SEC-6

Insufficient Credential Hygiene

CICD-SEC-7

Insecure System Configuration

CICD-SEC-8

Ungoverned Usage of Third-Party Services

CICD-SEC-9

Improper Artifact Integrity Validation

CICD-SEC-10

Insufficient Logging and Visibility

OWASP Top 10 CI/CD security risks

CICD-SEC-1 Insufficient Flow Control Mechanisms	**CICD-SEC-2** Inadequate Identity and Access Management	CICD-SEC-3 Dependency Chain Abuse	CICD-SEC-4 Poisoned Pipeline Execution (PPE)	CICD-SEC-5 Insufficient PBAC (Pipeline-Based Access Controls)
CICD-SEC-6 Insufficient Credential Hygiene	CICD-SEC-7 Insecure System Configuration	CICD-SEC-8 Ungoverned Usage of Third-Party Services	CICD-SEC-9 Improper Artifact Integrity Validation	CICD-SEC-10 Insufficient Logging and Visibility

OWASP Top 10 CI/CD security risks

CICD-SEC-1 Insufficient Flow Control Mechanisms	CICD-SEC-2 Inadequate Identity and Access Management	**CICD-SEC-3** Dependency Chain Abuse	CICD-SEC-4 Poisoned Pipeline Execution (PPE)	CICD-SEC-5 Insufficient PBAC (Pipeline-Based Access Controls)
CICD-SEC-6 Insufficient Credential Hygiene	CICD-SEC-7 Insecure System Configuration	CICD-SEC-8 Ungoverned Usage of Third-Party Services	CICD-SEC-9 Improper Artifact Integrity Validation	CICD-SEC-10 Insufficient Logging and Visibility

OWASP Top 10 CI/CD security risks

CICD-SEC-1 Insufficient Flow Control Mechanisms	**CICD-SEC-2** Inadequate Identity and Access Management	**CICD-SEC-3** Dependency Chain Abuse	**CICD-SEC-4** Poisoned Pipeline Execution (PPE)	**CICD-SEC-5** Insufficient PBAC (Pipeline-Based Access Controls)
CICD-SEC-6 Insufficient Credential Hygiene	**CICD-SEC-7** Insecure System Configuration	**CICD-SEC-8** Ungoverned Usage of Third-Party Services	**CICD-SEC-9** Improper Artifact Integrity Validation	**CICD-SEC-10** Insufficient Logging and Visibility

OWASP Top 10 CI/CD security risks

CICD-SEC-1 Insufficient Flow Control Mechanisms	CICD-SEC-2 Inadequate Identity and Access Management	CICD-SEC-3 Dependency Chain Abuse	CICD-SEC-4 Poisoned Pipeline Execution (PPE)	**CICD-SEC-5** Insufficient PBAC (Pipeline-Based Access Controls)
CICD-SEC-6 Insufficient Credential Hygiene	CICD-SEC-7 Insecure System Configuration	CICD-SEC-8 Ungoverned Usage of Third-Party Services	CICD-SEC-9 Improper Artifact Integrity Validation	CICD-SEC-10 Insufficient Logging and Visibility

OWASP Top 10 CI/CD security risks

CICD-SEC-1 Insufficient Flow Control Mechanisms	**CICD-SEC-2** Inadequate Identity and Access Management	**CICD-SEC-3** Dependency Chain Abuse	**CICD-SEC-4** Poisoned Pipeline Execution (PPE)	**CICD-SEC-5** Insufficient PBAC (Pipeline-Based Access Controls)
CICD-SEC-6 Insufficient Credential Hygiene	**CICD-SEC-7** Insecure System Configuration	**CICD-SEC-8** Ungoverned Usage of Third-Party Services	**CICD-SEC-9** Improper Artifact Integrity Validation	**CICD-SEC-10** Insufficient Logging and Visibility

OWASP Top 10 CI/CD security risks

CICD-SEC-1 Insufficient Flow Control Mechanisms	CICD-SEC-2 Inadequate Identity and Access Management	CICD-SEC-3 Dependency Chain Abuse	CICD-SEC-4 Poisoned Pipeline Execution (PPE)	CICD-SEC-5 Insufficient PBAC (Pipeline-Based Access Controls)
CICD-SEC-6 Insufficient Credential Hygiene	**CICD-SEC-7** Insecure System Configuration	CICD-SEC-8 Ungoverned Usage of Third-Party Services	CICD-SEC-9 Improper Artifact Integrity Validation	CICD-SEC-10 Insufficient Logging and Visibility

OWASP Top 10 CI/CD security risks

CICD-SEC-1 Insufficient Flow Control Mechanisms	**CICD-SEC-2** Inadequate Identity and Access Management	**CICD-SEC-3** Dependency Chain Abuse	**CICD-SEC-4** Poisoned Pipeline Execution (PPE)	**CICD-SEC-5** Insufficient PBAC (Pipeline-Based Access Controls)
CICD-SEC-6 Insufficient Credential Hygiene	**CICD-SEC-7** Insecure System Configuration	**CICD-SEC-8** Ungoverned Usage of Third-Party Services	**CICD-SEC-9** Improper Artifact Integrity Validation	**CICD-SEC-10** Insufficient Logging and Visibility

OWASP Top 10 CI/CD security risks

CICD-SEC-1 Insufficient Flow Control Mechanisms	**CICD-SEC-2** Inadequate Identity and Access Management	**CICD-SEC-3** Dependency Chain Abuse	**CICD-SEC-4** Poisoned Pipeline Execution (PPE)	**CICD-SEC-5** Insufficient PBAC (Pipeline-Based Access Controls)
CICD-SEC-6 Insufficient Credential Hygiene	**CICD-SEC-7** Insecure System Configuration	**CICD-SEC-8** Ungoverned Usage of Third-Party Services	**CICD-SEC-9** Improper Artifact Integrity Validation	**CICD-SEC-10** Insufficient Logging and Visibility

OWASP Top 10 CI/CD security risks

CICD-SEC-1 Insufficient Flow Control Mechanisms	**CICD-SEC-2** Inadequate Identity and Access Management	**CICD-SEC-3** Dependency Chain Abuse	**CICD-SEC-4** Poisoned Pipeline Execution (PPE)	**CICD-SEC-5** Insufficient PBAC (Pipeline-Based Access Controls)
CICD-SEC-6 Insufficient Credential Hygiene	**CICD-SEC-7** Insecure System Configuration	**CICD-SEC-8** Ungoverned Usage of Third-Party Services	**CICD-SEC-9** Improper Artifact Integrity Validation	**CICD-SEC-10** Insufficient Logging and Visibility

Chalk talk challenge

How do we build a more secure software build and release pipeline with mitigations against the Top 10 CI/CD risks using primarily AWS services?

Session summary

- Enforce least privilege across CI/CD infrastructure
- Implement effective secrets management
- Understand both the security “OF” and “IN” the pipeline
- Understand shared responsibility and managed pipelines
- Monitor CI/CD infrastructure

Mitigating OWASP Top 10 CI/CD Security Risks using AWS services

Additional resources

OWASP Top 10 CI/CD
Security Risks

AWS Well-architected Framework:
Application Security Pillar

Thank you!

Please complete the session survey in the mobile app

Daniel Begimher
in/begimher
dbbegimh@amazon.com

Patrick Gaw
in/patrick-gaw
patgaw@amazon.com