Beyond Code:
Reinforcing CI/CD Pipelines Against Emerging Threats

Farshad Abasi

Hello World.

Introductions

Embarking on a Secure CI/CD Journey

Introduction to the secure CI/CD journey.

Importance of security in CI/CD pipelines.

Objectives of today's session.

Your Navigator in the CI/CD Security Realm

FARSHAD ABASI

- 27+ years in software and cybersecurity.
- CEO of Forward Security + Eureka DevSecOps - specializing in AppSec, CloudSec, and DevSecOps.
- Former Principal Security Architect at HSBC Global, Head of IT Security for Canada, and AppSec leader
- Instructor at BCIT, shaping future cybersecurity experts.
- Contributor to BSides Vancouver and OWASP
- Academic and professional background in Computer Science, with various security certifications.

The Map Ahead: Today's Expedition Overview

- CI/CD SECURITY LANDSCAPE.
- DEEP DIVE INTO TOP 10 CI/CD RISKS.
- KEY TAKEAWAYS AND Q&A.

FWDSEC {i} eureka

The Evolving CI/CD Landscape

The CI/CD Universe: Expanding Frontiers

- CI/CD as the backbone of modern software development.
- Evolution and expansion of CI/CD technologies.
- Challenges and opportunities in the current CI/CD landscape.

When the Walls Fell: Learning from CI/CD Breaches

SolarWinds: A supply chain compromise.

Codecov: Secrets exposure through CI tools.

Dependency Confusion: Exploiting package namespace confusion.

Navigating the OWASP Top 10 CI/CD Security Risks

Charting the Hazards:
OWASP Top 10 CI/CD Security Risks

- Introduction to OWASP Top 10 CI/CD Risks.
- Focus on the impact of these risks on CI/CD pipelines.
- Mitigation strategies for common CI/CD security risks.

Insufficient Flow Control Mechanisms: Navigating the Rapids

1

Flow Control: Why It Matters?

Importance of vetting changes in CI/CD pipelines.

Lessons from the Front Lines

SolarWinds and Codecov as wake-up calls.

Tightening the Reins

Practical steps for better security.

FWDSEC eureka

Inadequate Identity and Access Management: Guarding the Gates

2

The PHP Git Compromise

A breach due to exposed user database and weak server-side IAM.

Action Steps Post-Breach

PHP's transition to stronger IAM measures on GitHub.

IAM Best Practices

Implementing strict access, strong authentication, and least privilege.

Dependency Chain Abuse: The Weakest Link

3

Targeting Trust in Dependencies

Challenges in safeguarding against dependency confusion and hijacking techniques.

High-Profile Hijinks

Examining incidents like the NPM package breaches affecting major tech firms.

Defensive Detailing

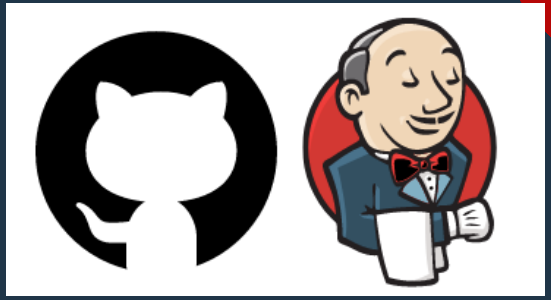
Enforcing internal repository use, verifying checksums and signatures, and locking down package versions.

Poisoned Pipeline Execution (PPE): The Trojan Horse

4

Understanding PPE: Direct and indirect methods of pipeline poisoning.

Guarding the Gates: Code review processes and CI/CD configuration security.



Illustrative Incidents: GitHub Actions and Jenkins vulnerabilities exploited.

Insufficient PBAC (Pipeline-Based Access Controls): Loose Ends

5

PBAC Essentials

Critical for safeguarding CI/CD processes by regulating who can perform what actions within the pipeline.

Distinguishing PBAC from IAM

IAM focuses on user identity and access management across systems, PBAC controls access within the CI/CD pipelines.

Case Study - The Codecov Breach

Intersection of PBAC and IAM vulnerabilities, highlighting the need for solid access controls both in IAM and within pipeline processes.

Insufficient Credential Hygiene: Cleaning Up Our Act

6

Credential Sprawl and Its Perils

Highlighting the widespread issue of poorly managed secrets across CI/CD environments.

Codecov and Travis CI Incidents

Analyzing breaches that underscore the critical need for stringent credential hygiene.

Fortifying Our Defenses

Practical measures for enhancing credential security in CI/CD pipelines.

Insecure System Configuration: Achilles' Heel

7

The Landscape of Misconfigurations

Exploiting default settings and overlooked updates.

Nissan's Open Door

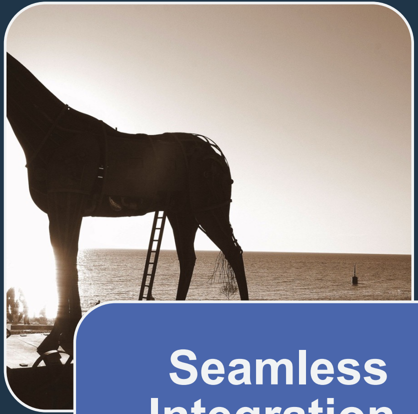
How a misconfigured Git server led to a wide-scale data leak.

Bolstering Our Defenses

Strategies for tightening system configurations across the CI/CD pipeline.

Ungoverned Usage of 3rd Party Services: Stranger Danger

8



Seamless Integration, Hidden Risks

The allure and risks of integrating third-party services into CI/CD pipelines.

The DeepSource Incident

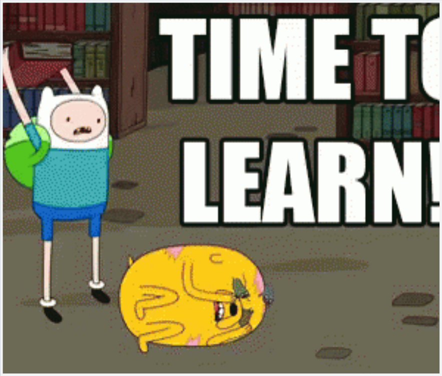
A breach through a GitHub engineer's account leads to widespread codebase access.

Safeguarding Against Third-Party Threats

Strategies for secure integration of external services.

Improper Artifact Integrity Validation: Trust but Verify

9



Learning from Codecov

Transforming a breach into a learning opportunity.

Evolving Validation Practices

Moving beyond the basics to continuous defense.

Strengthening Our Defenses

Implementing concrete steps for robust artifact security.

Insufficient Logging and Visibility: Flying Blind

10

The Imperative of Detection

- The critical role of logging in uncovering hidden threats.

Enhancing Visibility

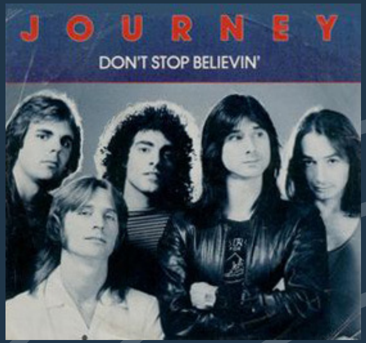
- Strategies for shedding light on dark corners of CI/CD pipelines.

Learning from the Field

- Insights from Travis CI and PHP Git Server incidents.

Conclusion and Q&A

The Treasure Map: Key Takeaways and Next Steps



Recap of Our CI/CD Security Journey

A synthesis of critical insights from notable breaches including SolarWinds, Codecov, Travis CI, Amazon, and Slack, alongside the defensive strategies discussed.

Navigating OWASP's Guidance

Leveraging the OWASP Top 10 CI/CD Security Risks to identify and mitigate the most significant vulnerabilities in our pipelines.

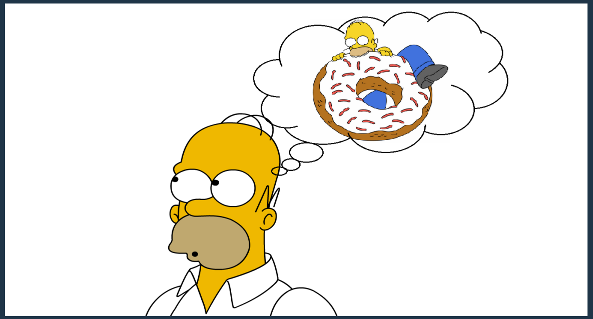
Concrete Actions for Pipeline Security

Initiating comprehensive audits, strengthening access controls, ensuring artifact integrity, and bolstering logging and monitoring practices.

Embracing Continuous Improvement

Recognizing that the journey towards secure CI/CD environments is ongoing, fueled by continuous learning, adaptation, and vigilance against evolving threats.

Open Seas:
Navigating Your Questions



Your Turn to Dive In

Ready for all your burning questions!

Farshad Abasi | f.abasi@fwdsec.com

www.forwardsecurity.com /
www.eurekadevsecops.com

Thank You

Farshad Abasi

f.abasi@fwdsec.com

www.forwardsecurity.com /
www.eurekadevsecops.com

FWDSEC eureka