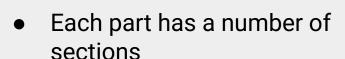


# Security Training for Developers

Part 2: Section 4: Dependency Management

#### **About This Training**

- For Developers
- Designed in three parts
  - Foundations and Systems Security (for all Contributors)
  - Vulnerability
    Management (for all Contributors)
  - Advanced Subjects (for Committers and future Committers)



- Typically 15 minutes of study
- Choose what matches your needs
- Content
  - Videos (live or pre-recorded)
  - Readings
  - Exercises



# **Evaluating risk of dependencies**





Unfixed vulnerabilities

Maintenance

Code integrity



## **Examples of past issues with dependencies**

- XZ compression library
  - Malicious co-maintainer included a backdoor
  - Single-maintainer project, social engineering attack
- Log4j logging library
  - A bug in a popular library, that was not considered security-related

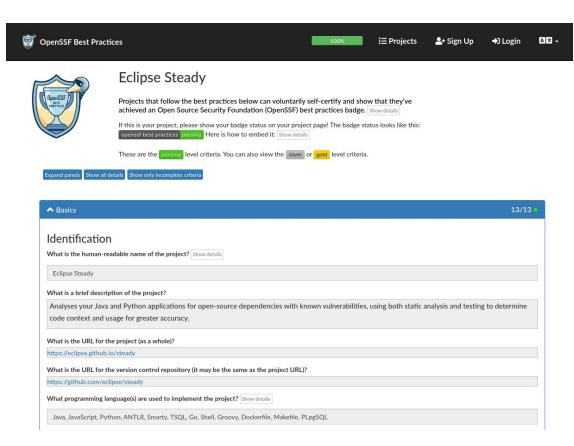


#### **Common questions**

- Is the project active?
- How big is the committer/maintainer team?
- Who can push to the repository?
- How do they protect code integrity?
- Do they provide stable APIs (Application Programming Interface) and ABI (Application Binary Interface)?

### **Evaluating dependencies: Best Practices Badge**

- Human-filled
- https://www.bestpractic es.dev/en/projects



#### **Tools**



#### **Dependabot**

- Github-native tool to help developers automatically manage and secure their project dependencies
  - Reduces risk from vulnerable dependencies
  - Ensures up-to-date software
  - Minimizes overhead of manual dependency management
- Main features
  - Security Alerts
  - 2. Security Updates
  - 3. Version Updates

#### 1. Security Alerts

- Dependabot creates alerts for vulnerabilities affecting dependencies
- Triage can be manual or automated
- Resolution can be dismissed or fixed
- Notification preference can be customised

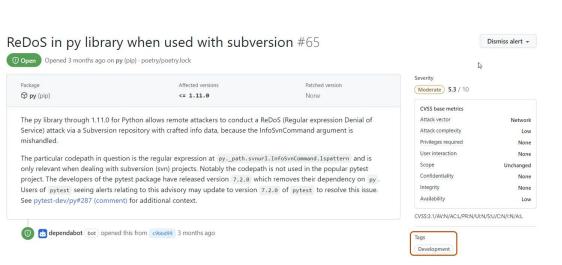
To enable Dependabot alerts for projects via Otterdog, set Repository Settings dependabot\_alerts\_enabled in the repository config file from .eclipsefdn.

To enables Dependabot alerts by default for new repositories at organization level, set <u>Organization Settings</u>

dependabot\_alerts\_enabled\_for\_new\_repositories.

#### What is a Security Alert?

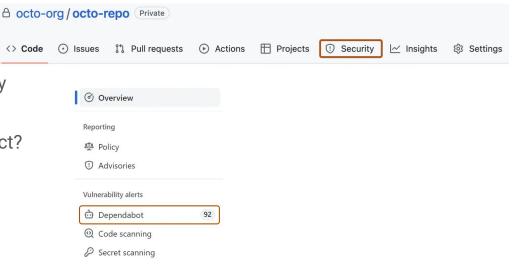
- Package Name
- Vulnerability ID
  - Github Advisory (GHSA-xxxx)
  - CVE Identifier (CVE-2024-xxxx)
- Severity
  - Low/Moderate/High/Critical
- Affected version range
- Patched version range
- Dependency type
- Manifest file path
- Reference links



Source: https://docs.github.com/en/code-security/dependabot/dependabot-alerts

#### **How to triage a Security Alert?**

- Asses severity
  - Focus first on High or Critical alerts
  - Checks CVSS vector and exploitability
- Check usage
  - Is the vulnerability affecting my project?
- Test patched version
  - Create a test branch with patched version
  - Run existing tests & CI workflows
- PR update and merge





Source: https://docs.github.com/en/code-security/dependabot/dependabot-alerts

#### **How to triage a Security Alert?**

- Asses severity
  - Focus first on High or Critical alerts
  - Checks CVSS vector and exploitability
- Check usage
  - Is this vulnerability affecting my project?
- Test patched version
  - Create a test branch with patched version
  - Run existing tests & Cl workflows
- PR update and merge

OR use **Dependabot Security Updates** 



Source: https://docs.github.com/en/code-security/dependabot/dependabot-alerts

#### 2. Security Updates

- Automated PRs that help you update vulnerable dependencies
- Dependabot:
  - Checks if an update does not disrupt the dependency graph
  - PR to update to the minimum version with a patch
  - Links the PR to the Security Alert

To enable Dependabot alerts for projects via Otterdog, set Repository Settings dependabot\_security\_updates\_enabled in the repository config file from .eclipsefdn.

To enable Dependabot alerts by default for new repositories at organization level, set <a href="Organization Settings">Organization Settings</a>

dependabot\_security\_updates\_enabled\_for\_new\_repositories.

#### 3. Version Updates

- Not directly related to security issues
- Automatically checks for new versions of project dependencies
- Creates a PR to bump the version when a new one is released
- Can be customized
  - Frequency
  - Target specific ecosystems
  - Update strategy

#### Readings

- Securing Development Branches Best Practices: <a href="https://eclipse-csi.github.io/security-handbook/developer/branches.html">https://eclipse-csi.github.io/security-handbook/developer/branches.html</a>
- Dependabot explained: <u>https://eclipse-csi.github.io/security-handbook/developer/branches.html</u>
- Dependabot documentation:
  <a href="https://docs.github.com/en/code-security/dependabot">https://docs.github.com/en/code-security/dependabot</a>
- Mend Renovate explained: <u>https://eclipse-csi.github.io/security-handbook/developer/branches.html#mend-renovate</u>
- Mend Renovate documentation: <a href="https://docs.renovatebot.com/">https://docs.renovatebot.com/</a>



Thank you!