



Security Training for ●●●●●●

Developers

Part 2: Section 1: Vulnerability Management Introduction

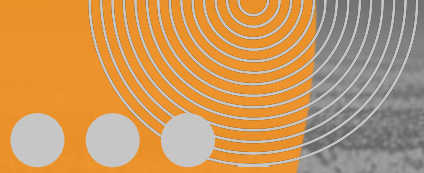


About This Training

- 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)

- Each part has a number of sections
 - Typically 15 minutes of study
 - Choose what matches your needs
- Content
 - Videos (live or pre-recorded)
 - Readings
 - Exercises





What is a vulnerability?



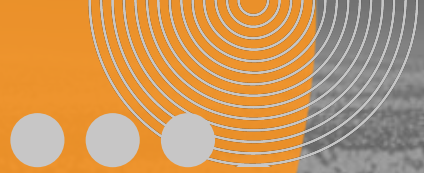
Security Properties

- **Confidentiality**
- **Integrity**
- **Availability**

Vulnerability definition



- *An instance of one or more weaknesses in a Product that **can be exploited**, causing a negative impact to **confidentiality, integrity, or availability**; a set of conditions or behaviors that allows the violation of an explicit or implicit security policy. (CVE Programme Glossary <https://www.cve.org/ResourcesSupport/Glossary#glossaryVulnerability>)*
- *'vulnerability' means a weakness, susceptibility or flaw of a product with digital elements that can be exploited by a cyber threat; (The Cyber Resilience Act, Article 3)*



Exercise

Vulnerability 1: true or false?



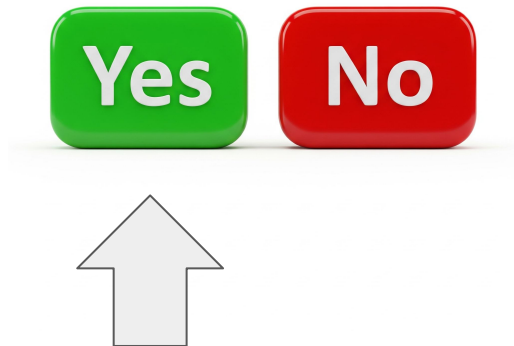
- In a web application, a user can log in to any account by using the password '12345', instead of the actual password. This additional password cannot be disabled by a configuration option.



Vulnerability 1: true or false?



- In a web application, a user can log in to any account by using the password '12345', instead of the actual password. This additional password cannot be disabled by a configuration option.



Vulnerability 2: true or false?



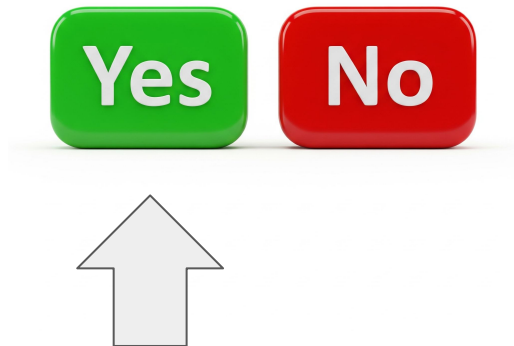
- A web server crashes when receiving a GET request of a specific URL with a set of specific parameters. The service needs to be restarted to function.



Vulnerability 2: true or false?



- A web server crashes when receiving a GET request of a specific URL with a set of specific parameters. The service needs to be restarted to function.



Vulnerability 3: true or false?



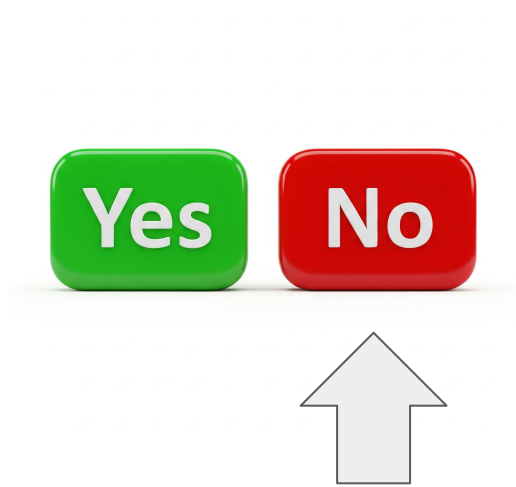
- In a text editor, the text color in one of the windows makes it very hard to read.

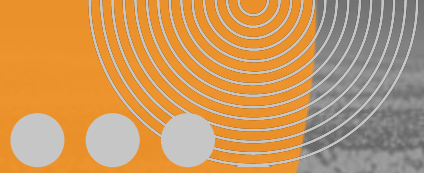


Vulnerability 3: true or false?



- In a text editor, the text color in one of the windows makes it very hard to read.





The vulnerability handling ecosystem

CVE (Common Vulnerabilities and Exposures)



- The biggest vulnerability database
 - Scope: known vulnerabilities in all products (commercial, open source...)
 - Data since 1999
- Assigns CVE IDs, like CVE-1900-1234
 - The entry contains a description, possible vendor, severity information
 - Various format over the years, currently all data available in a JSON format
<https://github.com/CVEProject/cvelistV5>
 - Data quality varies
- The Eclipse Foundation assigns CVE IDs
 - Technically, the EF is a CNA - CVE Numbering Authority
- Recent issues
 - Financed by US government
 - Funding issue memo leaked on April 15, 2025 - issue resolved since, but community trust issue

NVD (National Vulnerability Database)



- Augments CVE with information like:
 - Machine-readable product/vendor information (necessary for automatic scanners)
 - Severity information (for prioritization purposes)
- Currently preferred source for vulnerability scanners
- Recent issues
 - Stopped adding new entries in February 2024, restarted since
 - But still an important backlog

Other vulnerability databases



- GitHub Advisories <https://github.com/advisories>
 - Generated from GitHub private advisories
- OSV for open source projects only <https://osv.dev/>
 - Machine-readable format by default
 - Supported by Google
- EUVD (new, in beta) <https://euvd.enisa.europa.eu/>
 - Currently assembling existing sources
 - Will be used in the context of the CRA (Cyber Resilience Act)

How to read a CVE entry (1)



CVE-2025-4447 PUBLISHED

[View JSON](#) | [User Guide](#)

[Collapse all](#)

Required CVE Record Information

CNA: Eclipse Foundation

Published: 2025-05-09 **Updated:** 2025-05-09

Title: Buffer Overflow In Eclipse OpenJ9

Description

In Eclipse OpenJ9 versions up to 0.51, when used with OpenJDK version 8 a stack based buffer overflow can be caused by modifying a file on disk that is read when the JVM starts.

CWE 1 Total

[Learn more](#)

- [CWE-121: CWE-121: Stack-based Buffer Overflow](#)

CVSS 1 Total

[Learn more](#)

Score	Severity	Version	Vector String
7.0	HIGH	4.0	CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/VC:L/VI:H/VA:H/SC:H/SI:N/SA:N

From:
<https://www.cve.org/cverecord?id=CVE-2025-4447>

How to read a CVE entry (2)



CVSS 1 Total

[Learn more](#)

Score	Severity	Version	Vector String
7.0	HIGH	4.0	CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/VC:L/VI:H/VA:H/SC:H/SI:N/SA:N

Product Status

[Learn more](#)

Vendor

Eclipse Foundation

Product

OpenJ9

Versions 1 Total

Default Status: unaffected

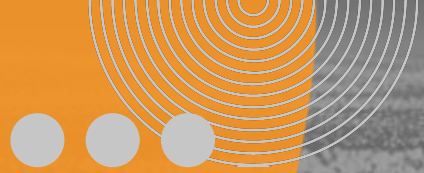
Affected

- affected from 0.8.0 through 0.49.0

References 2 Total

- <https://gitlab.eclipse.org/security/cve-assignment/-/issues/61>
- <https://github.com/eclipse-openj9/openj9/pull/21762>

From:
<https://www.cve.org/cverecord?id=CVE-2025-4447>



Vulnerability reporting

Who can report vulnerabilities?

- Security researchers
- Other developers
- Users
- YOU!



Reporting DOs



- Find a confidential way to contact the affected Project
 - A dedicated mailing list
 - A dedicated security bug tracker
 - GitHub Private advisories (if enabled)
 - Bug bounty program (if the Project has one)
- Send details helping to reproduce
 - The exact version
 - Same information as in a regular bug request
- Answer follow-up questions
- Talk about the issue publicly AFTER the Project has released a fix
 - Agree with them on the date

Reporting DON'Ts



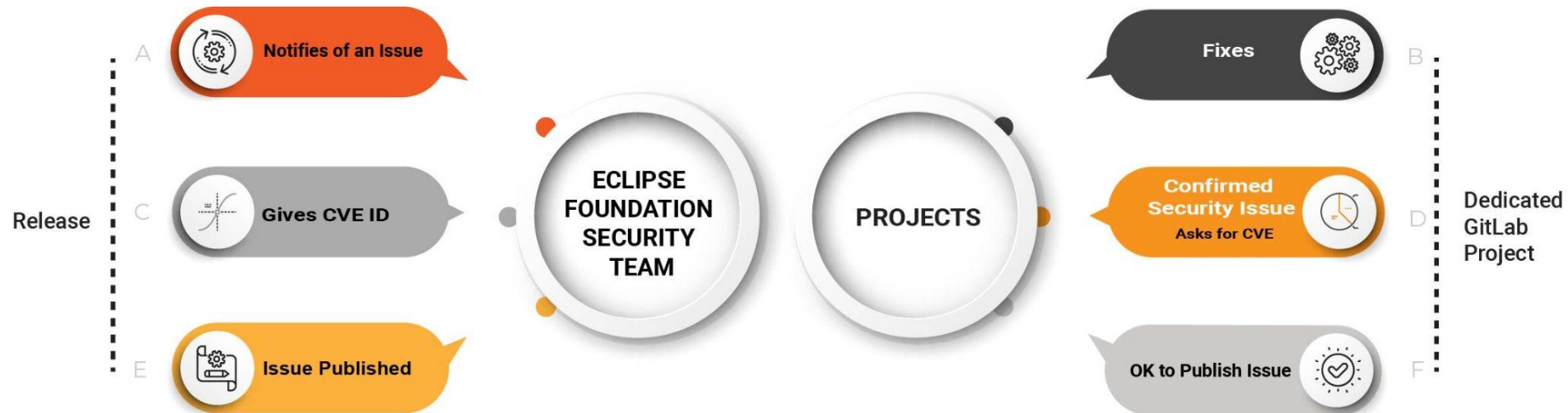
- Don't use public channels
 - Public mailing lists
 - IRC, Discord....
 - Public bug tracker issues
- Don't request payments for your discovery from open source projects
 - Except if a project has a paid bug bounty program
- Don't send results from automatic tools without verification
 - Verification of an issue requires precious time
- Don't talk about unfixed vulnerabilities
 - Before they get fixed

How to find out where to report: the SECURITY file



- The SECURITY(.txt, .md...) file
 - A common place to find the vulnerability reporting method
 - For source code repositories
- You may include other items
 - Supported versions
 - Links to security documentation of the Project
- Eclipse Foundation template if you do not have one:
 - <https://github.com/eclipse-csi/security-handbook/tree/main/templates>

Vulnerability Handling at EF



Quiz

Readings



- Eclipse Foundation Security Policy:
<https://www.eclipse.org/security/policy/>
- Eclipse Foundation Handbook on Vulnerability Management:
<https://www.eclipse.org/projects/handbook/#vulnerability>
- CVE Program Rules
<https://www.cve.org/resource/support/allresources/cnarules>
- Guide to implementing a coordinated vulnerability disclosure process for open source projects
<https://github.com/ossf/oss-vulnerability-guide/blob/main/maintainer-guide.md#readme>



Thank you!