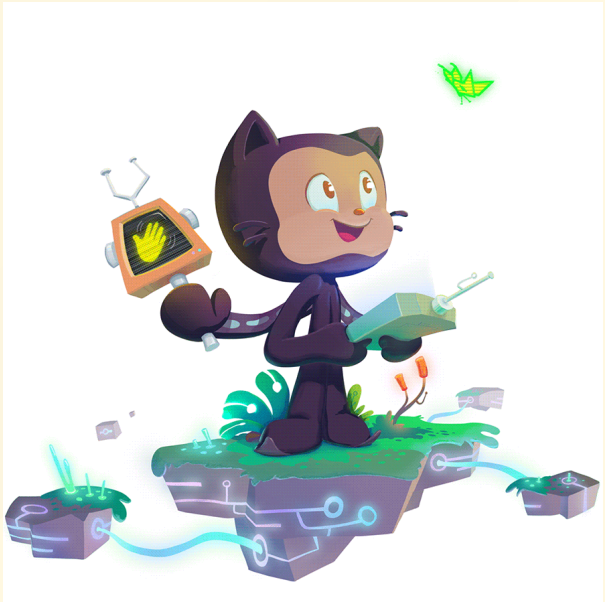
Open source + Security = ❤️

by Adrien Pessu (@adrienpessu) GitHub



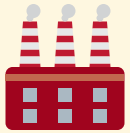
Introduction

Introduction

Introduction

Agenda

- 🏭 OWASP
- 📝 Open source security foundation
- ⚙️ MITRE
- 📺 How to open source

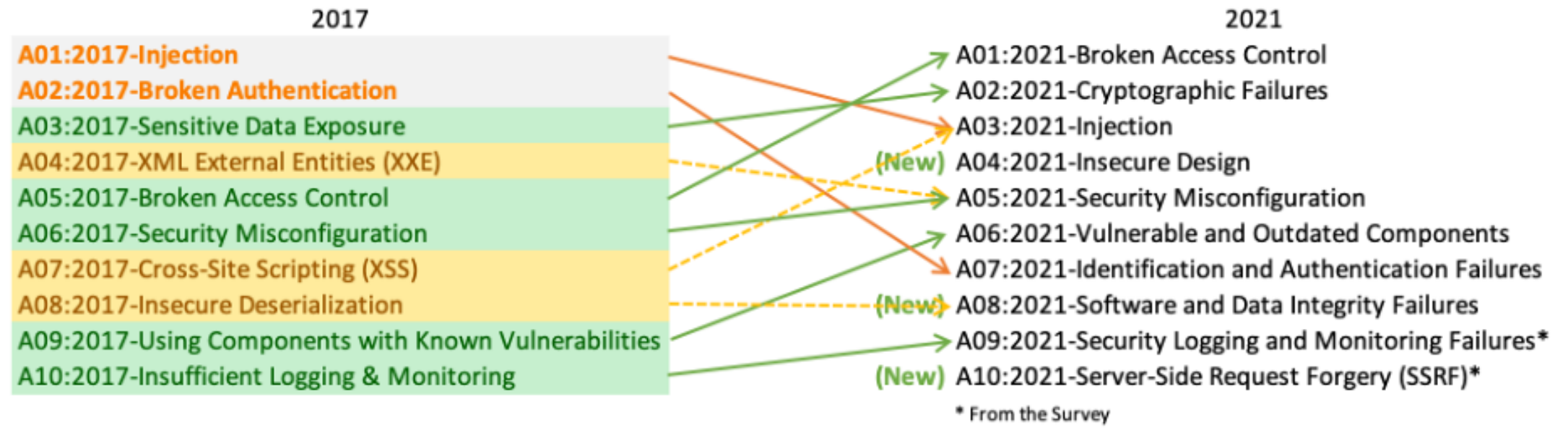


OWASP

The *Open Web Application Security Project*® (OWASP) is a **nonprofit foundation** that works to improve the security of software.

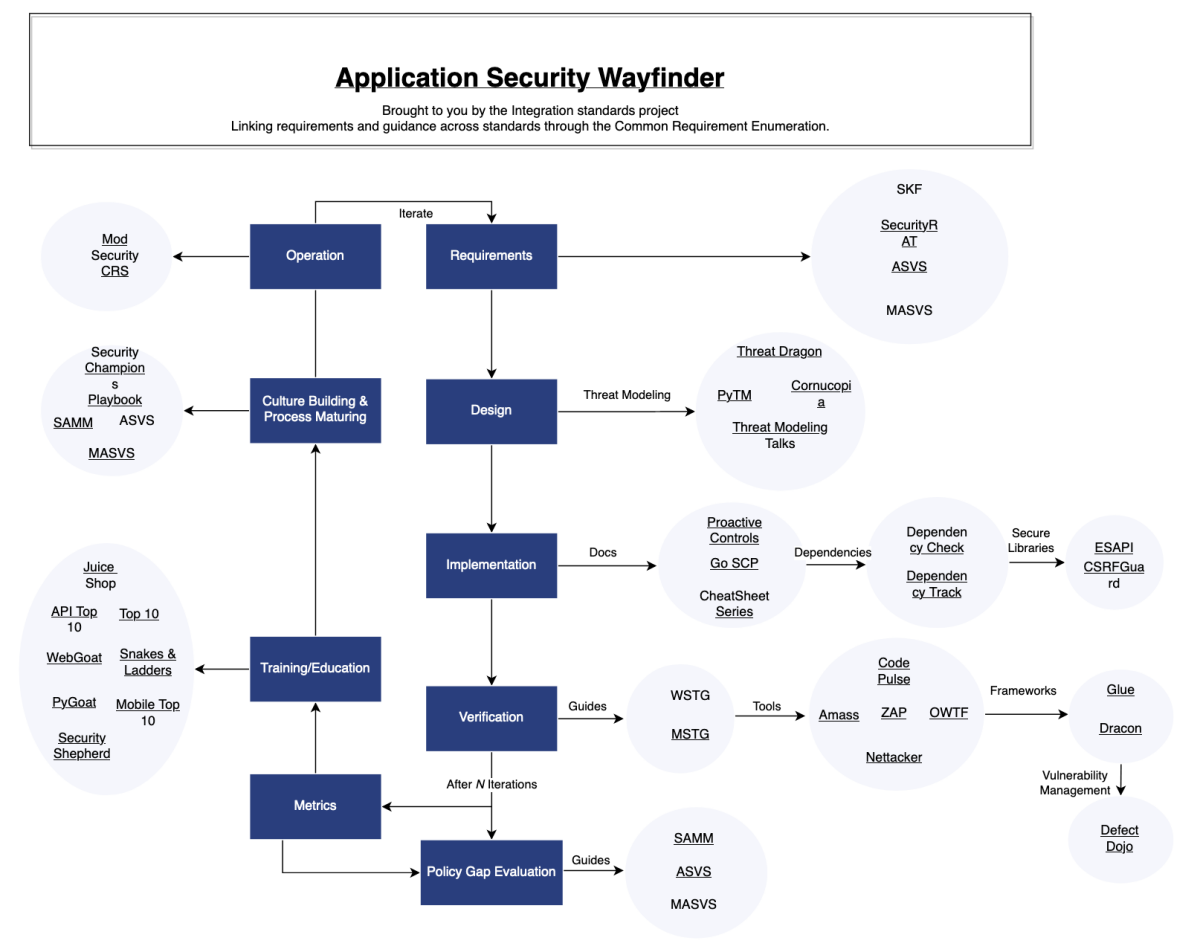
- open-source software projects,
- hundreds of local chapters worldwide,
- tens of thousands of members,
- and leading educational and training conferences

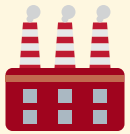
OWASP



https://owasp.org/Top10/fr/

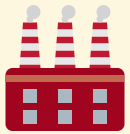
OWASP


Application Security Wayfinder
Brought to you by the Integration standards project
Linking requirements and guidance across standards through the Common Requirement Enumeration.
Iterate
Operation
Requirements
Mod Security CRS
SKF
SecurityRAT
ASVS
MASVS
Security Champions Playbook
SAMM
ASVS
MASVS
Culture Building & Process Maturing
Design
Threat Modeling
Threat Dragon
PyTM
Cornucopia
Threat Modeling Talks
Implementation
Docs
Proactive Controls
Go SCP
CheatSheet Series
Dependencies
Dependency Check
Dependency Track
Secure Libraries
ESAPI
CSRFGuard
Juice Shop
API Top 10
Top 10
WebGoat
Snakes & Ladders
PyGoat
Mobile Top 10
Security Shepherd
Training/Education
Verification
Guides
WSTG
MSTG
Tools
Code Pulse
Amass
ZAP
OWTF
Nettacker
Frameworks
Glue
Dracon
Vulnerability Management
Defect Dojo
After N Iterations
Metrics
Policy Gap Evaluation
Guides
SAMM
ASVS
MASVS



OWASP Dependency-check


```
dependency-check --project "myproject" --scan [project_path] --out
[output_path]
```

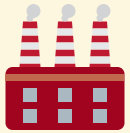
 OWASP AMASS

Network mapping of attack surfaces and external asset discovery.
Using Information Gathering Techniques :

- API : Pastebin, Twitter, GitHub, ...
- Certificates: Digitorus, FacebookCT, GoogleCT, ...
- DNS: Brute forcing, Reverse DNS sweeping, NSEC zone walking, ..

Routing, Scraping, Web Archives, WHOIS

```
amass enum -d example.com
```

 OWASP ZAP (Zed Attack Proxy)

- Proxy
- App Scanner

📝 Open source security foundation (OpenSSF)

Cross-industry forum for a collaborative effort to improve open source software security.

GitHub, Google, IBM, JPMorgan Chase, Microsoft, NCC Group, OWASP Foundation, Red Hat, HackerOne, Intel, Okta, Purdue, Uber, WhiteSource, and VMware.

📝 Open source security foundation (OpenSSF)

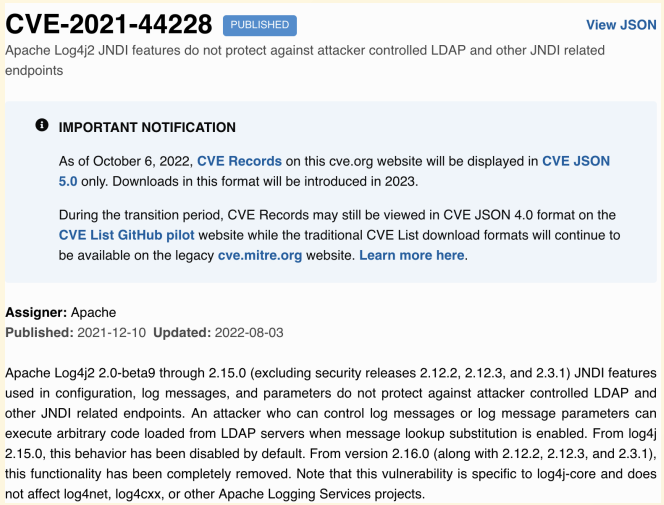
- Projects (like Sigstore, ...)
- Funding open source projects
- Free trainings
- Guides

⚙ MITRE

- American not-for-profit organization
- *"provide evidence-based, objective and nonpartisan insights for government policymaking"*

MITRE

- CVE : Common Vulnerabilities and Exposures



CVE-2021-44228 PUBLISHED View JSON

Apache Log4j2 JNDI features do not protect against attacker controlled LDAP and other JNDI related endpoints

IMPORTANT NOTIFICATION

As of October 6, 2022, **CVE Records** on this cve.org website will be displayed in **CVE JSON 5.0** only. Downloads in this format will be introduced in 2023.

During the transition period, CVE Records may still be viewed in CVE JSON 4.0 format on the **CVE List GitHub pilot** website while the traditional CVE List download formats will continue to be available on the legacy **cve.mitre.org** website. **Learn more here**.

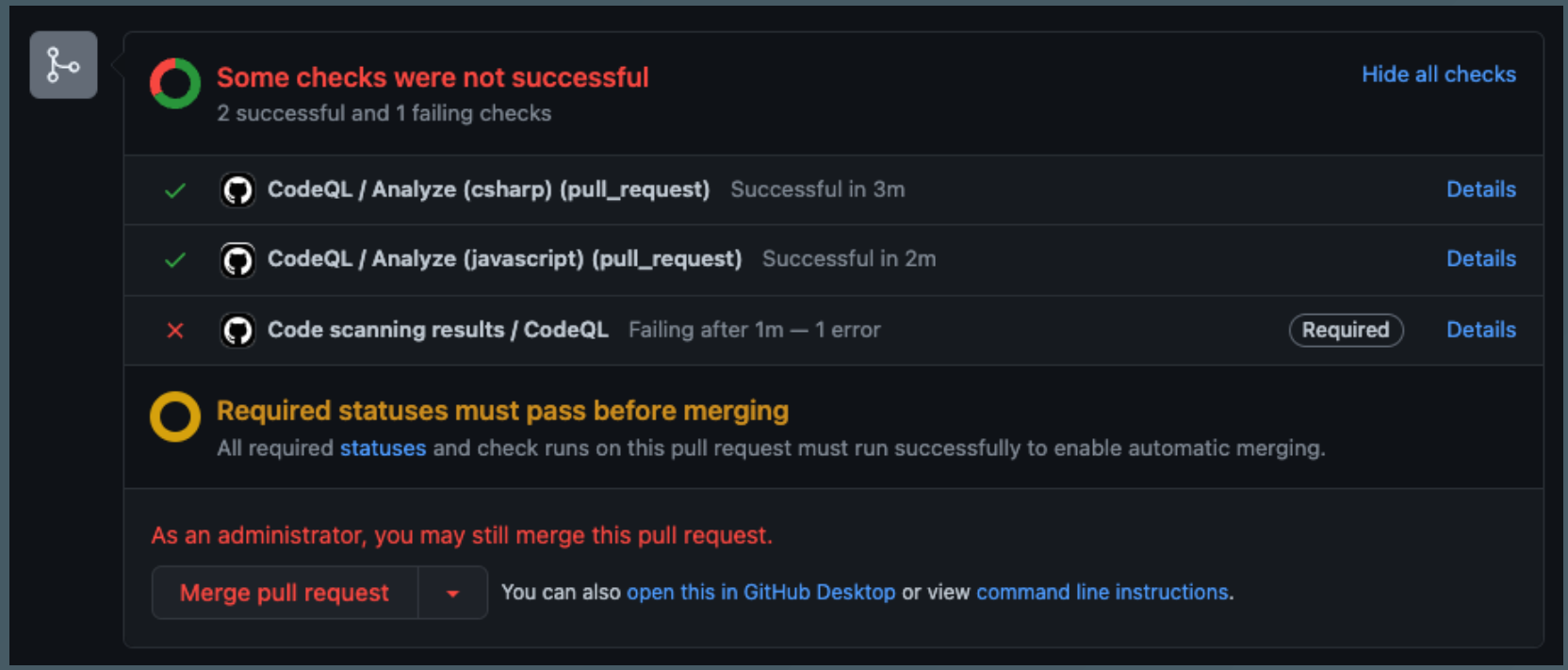
Assigner: Apache
Published: 2021-12-10 **Updated:** 2022-08-03

Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.

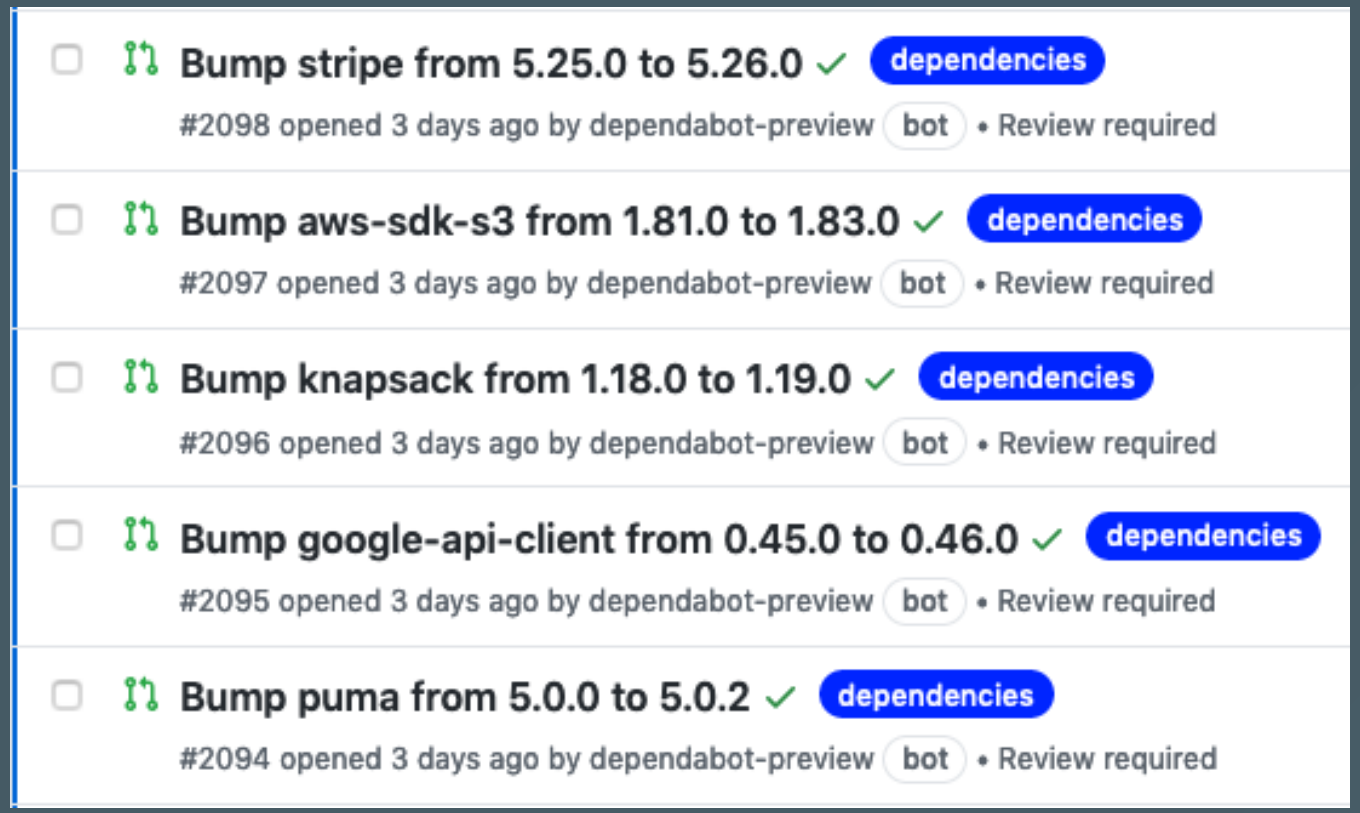
- ATT&CK : knowledge base of adversary tactics and techniques based on real-world observations

📺 How to open source but safely

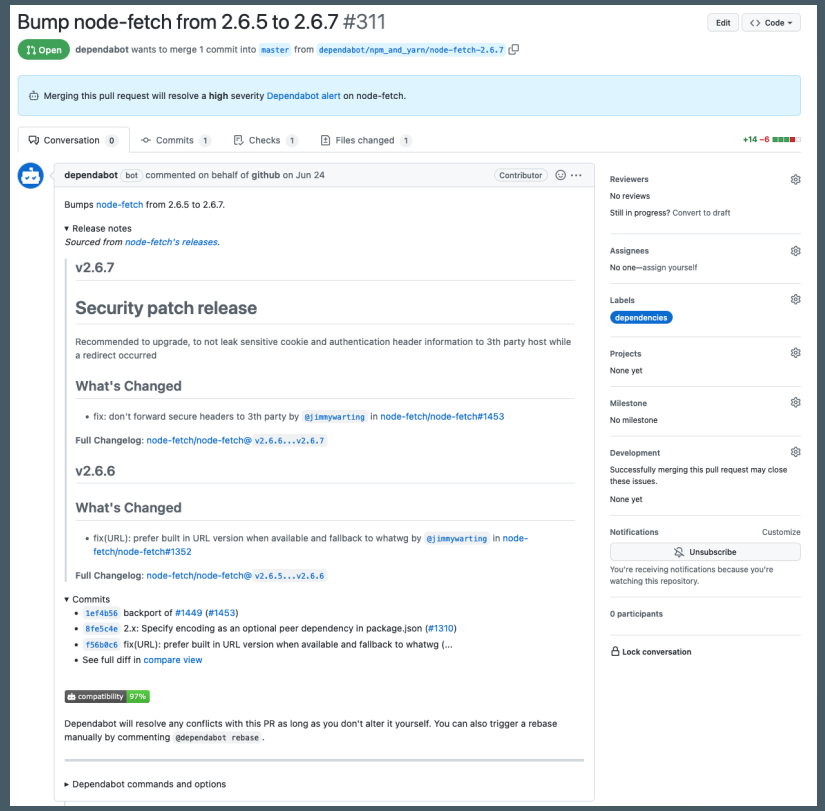
CodeQL && Secret scanning



📺 How to open source but safely



📺 How to open source but safely



Bump node-fetch from 2.6.5 to 2.6.7 #311

Edit Code

Open dependabot wants to merge 1 commit into master from dependabot/npm_and_yarn/node-fetch-2.6.7

Merging this pull request will resolve a high severity Dependabot alert on node-fetch.

Conversation 0 Commits 1 Checks 1 Files changed 1 +14 −6

dependabot bot commented on behalf of github on Jun 24 Contributor

Bumps node-fetch from 2.6.5 to 2.6.7.

▾ Release notes

Sourced from node-fetch's releases.

v2.6.7

Security patch release

Recommended to upgrade, to not leak sensitive cookie and authentication header information to 3th party host while a redirect occurred

What's Changed

- fix: don't forward secure headers to 3th party by @jimmywarting in node-fetch/node-fetch#1453

Full Changelog: node-fetch/node-fetch@ v2.6.6...v2.6.7

v2.6.6

What's Changed

- fix(URL): prefer built in URL version when available and fallback to whatwg by @jimmywarting in node-fetch/node-fetch#1352

Full Changelog: node-fetch/node-fetch@ v2.6.5...v2.6.6

▾ Commits

- 1ef4b56 backport of #1449 (#1453)
- 8fe5c4e 2.x: Specify encoding as an optional peer dependency in package.json (#1310)
- f56b0c6 fix(URL): prefer built in URL version when available and fallback to whatwg (...
- See full diff in compare view

compatibility 97%

Dependabot will resolve any conflicts with this PR as long as you don't alter it yourself. You can also trigger a rebase manually by commenting @dependabot rebase .

▸ Dependabot commands and options

Reviewers
No reviews
Still in progress? Convert to draft

Assignees
No one—assign yourself

Labels
dependencies

Projects
None yet

Milestone
No milestone

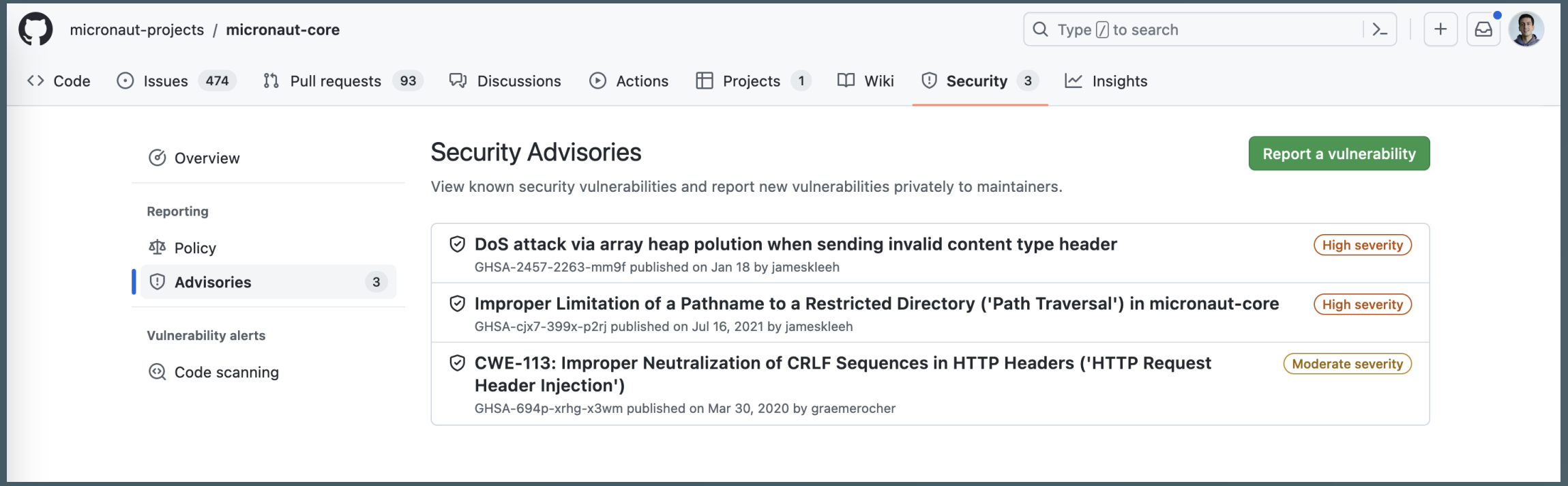
Development
Successfully merging this pull request may close these issues.
None yet

Notifications Customize
Unsubscribe
You're receiving notifications because you're watching this repository.

0 participants

Lock conversation

How to open source but safely



Conclusion

How to contribute ?

- Code
- Doc
- Talks
- Blog posts
- ...