SonarQube Report - Security HotSpots

Hotspot 1

Key: AZQXQr_8hzDY-Nmkkm6I

Component: digital-library:src/middlewares/userValidation.ts

Status: TO_REVIEW

Line: 15

Message: Make sure the regex used here, which is vulnerable to super-linear runtime due to backtracking, cannot lead to denial of service.

RuleKey: typescript:S5852

Full Scan ZAP Report - Alerts

Alert CSP: Wildcard Directive

PluginID: 10055

Risk code: 2

Confidence: 3

Risk description: Medium (High)

Alert Permissions Policy Header Not Set

PluginID: 10063

Risk code: 1

Confidence: 2

Risk description: Low (Medium)

Alert Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

PluginID: 10037

Risk code: 1

Confidence: 2

Risk description: Low (Medium)

Alert Storable and Cacheable Content

PluginID: 10049

Risk code: 0

Confidence: 2

Risk description: Informational (Medium)

API Scan ZAP Report - Alerts

Alert Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

PluginID: 10037

Risk code: 1

Confidence: 2

Risk description: Low (Medium)

Alert Unexpected Content-Type was returned

PluginID: 100001

Risk code: 1

Confidence: 3

Risk description: Low (High)

Alert X-Content-Type-Options Header Missing

PluginID: 10021

Risk code: 1

Confidence: 2

Risk description: Low (Medium)

Alert A Client Error response code was returned by the server

PluginID: 100000

Risk code: 0

Confidence: 3

Risk description: Informational (High)

Alert Storable and Cacheable Content

PluginID: 10049

Risk code: 0

Confidence: 2

Risk description: Informational (Medium)

Dependency check - vulnerabilities

Vulnerability 1

Dependency: path-to-regexp:0.1.10

Name: CVE-2024-52798

Severity: HIGH

CVSS Score: N/A

CWE: N/A

Description: path-to-regexp turns path strings into a regular expressions. In certain cases, path-to-regexp will output a regular expression that can be exploited to cause poor performance. The regular expression that is vulnerable to backtracking can be generated in the 0.1.x release of path-to-regexp. Upgrade to 0.1.12. This vulnerability exists because of an incomplete fix for CVE-2024-45296.

Vulnerability 2

Dependency: path-to-regexp:0.1.10

Name: GHSA-rhx6-c78j-4q9w

Severity: moderate

CVSS Score: N/A

CWE: N/A

Description: ### Impact

The regular expression that is vulnerable to backtracking can be generated in the 0.1.x release of `path-to-regexp`, originally reported in CVE-2024-45296

Patches

Upgrade to 0.1.12.

Workarounds

Avoid using two parameters within a single path segment, when the separator is not `.` (e.g. no `/:a-:b`). Alternatively, you can define the regex used for both parameters and ensure they do not overlap to allow backtracking.

References

- https://github.com/advisories/GHSA-9wv6-86v2-598j
- https://blakeembrey.com/posts/2024-09-web-redos/