How to read the report | Suppressing false positives | **Getting Help:** github issues

Sponsor

Project: juice-shop

Scan Information (show all):

- *dependency-check version*: 7.1.1
- *Report Generated On*: Mon, 27 Jun 2022 11:58:50 GMT
- *Dependencies Scanned*: 72 (72 unique)
- *Vulnerable Dependencies*: 6
- *Vulnerabilities Found*: 7
- *Vulnerabilities Suppressed*: 0
- ...

Summary

Display: Showing Vulnerable Dependencies (click to show all)

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count
express-jwt:0.1.3	cpe:2.3:a:auth0:express-jwt:0.1.3:*:*:*:*:*:*:*	pkg:npm/express-jwt@0.1.3	CRITICAL	1	Highest	9
hbs:4.2.0	cpe:2.3:a:hbs_project:hbs:4.2.0:*:*:*:*:*:*:*	pkg:npm/hbs@4.2.0	MEDIUM	1	Highest	6
jsonwebtoken:0.4.0	cpe:2.3:a:auth0:jsonwebtoken:0.4.0:*:*:*:*:*:*:*	pkg:npm/jsonwebtoken@0.4.0	CRITICAL	1	Highest	7
notevil:1.3.3	cpe:2.3:a:notevil_project:notevil:1.3.3:*:*:*:*:*:*:*	pkg:npm/notevil@1.3.3	MEDIUM	1	Highest	7
sanitize-html:1.4.2		pkg:npm/sanitize-html@1.4.2	MEDIUM	2		6
sqlite3:5.0.2		pkg:npm/sqlite3@5.0.2	HIGH	1		8

Dependencies

express-jwt:0.1.3

Description:

JWT authentication middleware.

File Path: /builds/itsec_ss22_csharps/cicdprojekt2/package.json?/express-jwt:0.1.3

Referenced In Project/Scope:juice-shop:14.0.1

Evidence

Identifiers

- pkg:npm/express-jwt@0.1.3 (*Confidence*:Highest)
- cpe:2.3:a:auth0:express-jwt:0.1.3:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2020-15084 suppress

In express-jwt (NPM package) up and including version 5.3.3, the algorithms entry to be specified in the configuration is not being enforced. When algorithms is not specified in the configuration, with the combination of jwks-rsa, it may lead to authorization bypass. You are affected by this vulnerability if all of the following conditions apply: - You are using express-jwt - You do not have **algorithms** configured in your express-jwt configuration. - You are using libraries such as jwks-rsa as the **secret**. You can fix this by specifying **algorithms** in the express-jwt configuration. See linked GHSA for

example. This is also fixed in version 6.0.0.

CWE-285 Improper Authorization

CVSSv2:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSSv3:
- Base Score: CRITICAL (9.1)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

References:
- CONFIRM - https://github.com/auth0/express-jwt/security/advisories/GHSA-6g6m-m6h5-w9gf
- MISC - https://github.com/auth0/express-jwt/commit/7ecab5f8f0cab5297c2b863596566eb0c019cdef
- OSSINDEX - [CVE-2020-15084] CWE-285: Improper Authorization
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-15084
- OSSIndex - https://github.com/auth0/express-jwt/security/advisories/GHSA-6g6m-m6h5-w9gf

Vulnerable Software & Versions:

- cpe:2.3:a:auth0:express-jwt:*:*:*:*:*:node.js:*:* versions up to (including) 5.3.3

hbs:4.2.0

Description:

Express.js template engine plugin for Handlebars

License:

MIT

File Path: /builds/itsec_ss22_csharps/cicdprojekt2/package.json?/hbs:^4.0.4

Referenced In Project/Scope:juice-shop:14.0.1

Evidence

Identifiers

- pkg:npm/hbs@4.2.0 (*Confidence*:Highest)
- cpe:2.3:a:hbs_project:hbs:4.2.0:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2021-32822 (OSSINDEX) suppress

The npm hbs package is an Express view engine wrapper for Handlebars. Depending on usage, users of hbs may be vulnerable to a file disclosure vulnerability. There is currently no patch for this vulnerability. hbs mixes pure template data with engine configuration options through the Express render API. By overwriting internal configuration options a file disclosure vulnerability may be triggered in downstream applications. For an example PoC see the referenced GHSL-2021-020.

CWE-200 Information Exposure

CVSSv2:
- Base Score: MEDIUM (5.3)
- Vector: /AV:N/AC:L/Au:/C:L/I:N/A:N

References:
- OSSINDEX - [CVE-2021-32822] CWE-200: Information Exposure
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-32822
- OSSIndex - https://github.com/advisories/GHSA-7f5c-rpf4-86p8
- OSSIndex - https://securitylab.github.com/advisories/GHSL-2021-020-pillarjs-hbs/
- OSSIndex - https://www.cybersecurity-help.cz/vdb/SB2021082412

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:*:hbs:4.2.0:*:*:*:*:*:*:*

jsonwebtoken:0.4.0

Description:

JSON Web Token implementation (symmetric and asymmetric)

License:

MIT

File Path: /builds/itsec_ss22_csharps/cicdprojekt2/package.json?/jsonwebtoken:0.4.0

Referenced In Project/Scope:juice-shop:14.0.1

Evidence

Identifiers

- pkg:npm/jsonwebtoken@0.4.0 (*Confidence*:Highest)
- cpe:2.3:a:auth0:jsonwebtoken:0.4.0:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2015-9235 suppress

In jsonwebtoken node module before 4.2.2 it is possible for an attacker to bypass verification when a token digitally signed with an asymmetric key (RS/ES family) of algorithms but instead the attacker send a token digitally signed with a symmetric algorithm (HS* family).

CWE-327 Use of a Broken or Risky Cryptographic Algorithm

CVSSv2:
- Base Score: HIGH (7.5)
- Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSSv3:
- Base Score: CRITICAL (9.8)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

References:
- MISC - https://auth0.com/blog/2015/03/31/critical-vulnerabilities-in-json-web-token-libraries/
- MISC - https://github.com/auth0/node-jsonwebtoken/commit/1bb584bc382295eeb7ee8c4452a673a77a68b687
- MISC - https://nodesecurity.io/advisories/17
- MISC - https://www.timmclean.net/2015/02/25/jwt-alg-none.html
- OSSINDEX - [sonatype-2015-0022] CWE-295: Improper Certificate Validation
- OSSIndex - https://www.npmjs.com/advisories/17

Vulnerable Software & Versions:

- cpe:2.3:a:auth0:jsonwebtoken:*:*:*:*:*:node.js:*:* versions up to (excluding) 4.2.2

notevil:1.3.3

Description:

Evalulate javascript like the built-in eval() method but safely

License:

MIT

File Path: /builds/itsec_ss22_csharps/cicdprojekt2/package.json?/notevil:^1.3.3

Referenced In Project/Scope:juice-shop:14.0.1

Evidence

Identifiers

- pkg:npm/notevil@1.3.3 (*Confidence*:Highest)
- cpe:2.3:a:notevil_project:notevil:1.3.3:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2021-23771 suppress

This affects all versions of package notevil; all versions of package argencoders-notevil. It is vulnerable to Sandbox Escape leading to Prototype pollution. The package fails to restrict access to the main context, allowing an attacker to add or modify an object's prototype. **Note:** This vulnerability derives from an incomplete fix in [SNYK-JS-NOTEVIL-608878](https://security.snyk.io/vuln/SNYK-JS-NOTEVIL-608878).

CWE-1321

CVSSv2:
- Base Score: MEDIUM (6.4)
- Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

References:
- MISC - https://snyk.io/vuln/SNYK-JS-ARGENCODERSNOTEVIL-2388587
- MISC - https://snyk.io/vuln/SNYK-JS-NOTEVIL-2385946
- OSSINDEX - [CVE-2021-23771] This affects all versions of package notevil; all versions of package argencoders-notevil. It is vulnerable to Sandbox Escape leading to Prototype pollution. The package fails to restrict access to the main context, allowing an attacker to add or modify an object's prototype. **Note:** This vulnerability derives from an incomplete fix in [SNYK-JS-NOTEVIL-608878](https://security.snyk.io/vuln/SNYK-JS-NOTEVIL-608878).
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-23771
- OSSIndex - https://github.com/mmckegg/notevil/blob/master/lib/primitives.js#L24

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:notevil_project:notevil:*:*:*:*:*:node.js:*:* versions up to (including) 1.3.3
- ...

sanitize-html:1.4.2

Description:

Clean up user-submitted HTML, preserving whitelisted elements and whitelisted attributes on a per-element basis

License:

MIT

File Path: /builds/itsec_ss22_csharps/cicdprojekt2/package.json?/sanitize-html:1.4.2

Referenced In Project/Scope:juice-shop:14.0.1

Evidence

Identifiers

- pkg:npm/sanitize-html@1.4.2 (*Confidence*:Highest)

Published Vulnerabilities

CVE-2016-1000237 (OSSINDEX) suppress

sanitize-html Sanitization not applied recursively - NPM

The software does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv3:
- Base Score: MEDIUM (6.3)
- Vector: CVSS:/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L

References:

- OSSINDEX - [sonatype-2014-0007] CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
- OSSIndex - https://github.com/punkave/sanitize-html/issues/29

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:*:sanitize-html:1.4.2:*:*:*:*:*:*:*

CVE-2021-26539 (OSSINDEX) suppress

Apostrophe Technologies sanitize-html before 2.3.1 does not properly handle internationalized domain name (IDN) which could allow an attacker to bypass hostname whitelist validation set by the "allowedIframeHostnames" option.

CWE-20 Improper Input Validation

CVSSv2:

- Base Score: MEDIUM (5.3)
- Vector: /AV:N/AC:L/Au:/C:N/I:L/A:N

References:

- OSSINDEX - [CVE-2021-26539] CWE-20: Improper Input Validation
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26539
- OSSIndex - https://github.com/apostrophecms/sanitize-html/blob/main/CHANGELOG.md#231-2021-01-22
- OSSIndex - https://github.com/apostrophecms/sanitize-html/pull/458

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:*:sanitize-html:1.4.2:*:*:*:*:*:*:*

sqlite3:5.0.2

Description:

Asynchronous, non-blocking SQLite3 bindings

License:

BSD-3-Clause

File Path: /builds/itsec_ss22_csharps/cicdprojekt2/package.json?/sqlite3:5.0.2

Referenced In Project/Scope:juice-shop:14.0.1

Evidence

Identifiers

- pkg:npm/sqlite3@5.0.2 (*Confidence*:Highest)

Published Vulnerabilities

CVE-2022-21227 (OSSINDEX) suppress

The package sqlite3 before 5.0.3 are vulnerable to Denial of Service (DoS) which will invoke the toString function of the passed parameter. If passed an invalid Function object it will throw and crash the V8 engine.

CWE-248 Uncaught Exception

CVSSv2:
- Base Score: HIGH (7.5)
- Vector: /AV:N/AC:L/Au:/C:N/I:N/A:H

References:
- OSSINDEX - [CVE-2022-21227] CWE-248: Uncaught Exception
- OSSIndex - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21227
- OSSIndex - https://github.com/TryGhost/node-sqlite3/pull/1450
- OSSIndex - https://github.com/advisories/GHSA-9qrh-qjmc-5w2p

Vulnerable Software & Versions (OSSINDEX):

- cpe:2.3:a:*:sqlite3:5.0.2:*:*:*:*:*:*:*

This report contains data retrieved from the National Vulnerability Database.
This report may contain data retrieved from the NPM Public Advisories.
This report may contain data retrieved from RetireJS.
This report may contain data retrieved from the Sonatype OSS Index.