Table of Contents

- Finding 36 - javascript.sequelize.security.audit.sequelize-injection-express.express-sequelize-injection

- Medium

  - Finding 37 - CVE-2025-8058 in libc6:2.36-9+deb12u10
  - Finding 38 - CVE-2025-9232 in libssl3:3.0.17-1~deb12u2
  - Finding 39 - GHSA-25hc-qcg6-38wj in socket.io:3.1.2
  - Finding 40 - GHSA-3j7m-hmh3-9jmp in sanitize-html:1.4.2
  - Finding 41 - GHSA-87vv-r9j6-g5qv in moment:2.0.0
  - Finding 42 - GHSA-8g4m-cjm2-96wq in notevil:1.3.3
  - Finding 43 - GHSA-952p-6rrq-rcjv in micromatch:3.1.10
  - Finding 44 - GHSA-cqmj-92xf-r6r9 in socket.io-parser:4.0.5
  - Finding 45 - GHSA-f5x3-32g6-xq36 in tar:4.4.19
  - Finding 46 - GHSA-fvqr-27wr-82fm in lodash:2.4.2
  - Finding 47 - GHSA-hjrf-2m68-5959 in jsonwebtoken:0.1.0
  - Finding 48 - GHSA-hjrf-2m68-5959 in jsonwebtoken:0.4.0
  - Finding 49 - GHSA-mjxr-4v3x-q3m4 in sanitize-html:1.4.2
  - Finding 50 - GHSA-p5gc-c584-jj6v in vm2:3.9.17
  - Finding 51 - GHSA-pfrx-2q88-qq97 in got:8.3.2
  - Finding 52 - GHSA-qhxp-v273-g94h in sanitize-html:1.4.2
  - Finding 53 - GHSA-qwph-4952-7xr6 in jsonwebtoken:0.1.0
  - Finding 54 - GHSA-qwph-4952-7xr6 in jsonwebtoken:0.4.0
  - Finding 55 - GHSA-r7qp-cfhv-p84w in engine.io:4.1.2
  - Finding 56 - GHSA-rjqq-98f6-6j3r in sanitize-html:1.4.2
  - Finding 57 - GHSA-rm97-x556-q36h in sanitize-html:1.4.2
  - Finding 58 - GHSA-rvg8-pwq2-xj7q in base64url:0.0.6
  - Finding 59 - GHSA-xc6g-ggrc-qq4r in sanitize-html:1.4.2
  - Finding 60 - generic.html-templates.security.unquoted-attribute-var.unquoted-attribute-var
  - Finding 61 - generic.html-templates.security.unquoted-attribute-var.unquoted-attribute-var
  - Finding 62 - generic.html-templates.security.unquoted-attribute-var.unquoted-attribute-var
  - Finding 63 - generic.html-templates.security.unquoted-attribute-var.unquoted-attribute-var
  - Finding 64 - javascript.express.security.audit.express-check-directory-listing.express-check-directory-listing
  - Finding 65 - javascript.express.security.audit.express-check-directory-listing.express-check-directory-listing
  - Finding 66 - javascript.express.security.audit.express-check-directory-listing.express-check-directory-listing
  - Finding 67 - javascript.express.security.audit.express-check-directory-listing.express-check-directory-listing
  - Finding 68 - javascript.express.security.audit.express-open-redirect.express-open-redirect
  - Finding 69 - javascript.express.security.audit.express-res-sendfile.express-res-sendfile
  - Finding 70 - javascript.express.security.audit.express-res-sendfile.express-res-sendfile
  - Finding 71 - javascript.express.security.audit.express-res-sendfile.express-res-sendfile
  - Finding 72 - javascript.express.security.audit.express-res-sendfile.express-res-sendfile
  - Finding 73 - javascript.express.security.audit.possible-user-input-redirect.unknown-value-in-redirect
  - Finding 74 - javascript.express.security.injection.raw-html-format.raw-html-format
  - Finding 75 - javascript.jsonwebtoken.security.jwt-hardcode.hardcoded-jwt-secret

- Finding 76 - javascript.lang.security.audit.unknown-value-with-script-tag.unknown-value-with-script-tag
- Finding 77 - javascript.lang.security.audit.unknown-value-with-script-tag.unknown-value-with-script-tag

- Low
  - Finding 78 - GHSA-pxg6-pf52-xh8x in cookie:0.4.2

- Info
  - Finding 79 - CVE-2010-4756 in libc6:2.36-9+deb12u10
  - Finding 80 - CVE-2018-20796 in libc6:2.36-9+deb12u10
  - Finding 81 - CVE-2019-1010022 in libc6:2.36-9+deb12u10
  - Finding 82 - CVE-2019-1010023 in libc6:2.36-9+deb12u10
  - Finding 83 - CVE-2019-1010024 in libc6:2.36-9+deb12u10
  - Finding 84 - CVE-2019-1010025 in libc6:2.36-9+deb12u10
  - Finding 85 - CVE-2019-9192 in libc6:2.36-9+deb12u10
  - Finding 86 - CVE-2022-27943 in gcc-12-base:12.2.0-14+deb12u1
  - Finding 87 - CVE-2022-27943 in libgcc-s1:12.2.0-14+deb12u1
  - Finding 88 - CVE-2022-27943 in libgomp1:12.2.0-14+deb12u1
  - Finding 89 - CVE-2022-27943 in libstdc++6:12.2.0-14+deb12u1
  - Finding 90 - CVE-2025-27587 in libssl3:3.0.17-1~deb12u2

Finding List

Critical

Finding 1 - GHSA-5mrr-rgp6-x4gr in marsdb:0.6.11

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Critical	N.A. / N.A.	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-5mrr-rgp6-x4gr']	88

Location

Component	Version
marsdb	0.6.11

File Path
/juice-shop/node_modules/marsdb/package.json

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: Command Injection in marsdb

Matcher: javascript-matcher

Package URL: pkg:npm/marsdb@0.6.11

References

Vulnerability Datasource: https://github.com/advisories/GHSA-5mrr-rgp6-x4gr

Finding 2 - GHSA-c7hr-j4mj-j2w6 in jsonwebtoken:0.1.0

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Critical (9.8)	41.15% / 97.31%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-c7hr-j4mj-j2w6', 'CVE-2015-9235']	27

Location

Component	Version
jsonwebtoken	0.1.0

File Path
/juice-shop/node_modules/express-jwt/node_modules/jsonwebtoken/package.json

CVSS v3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: Verification Bypass in jsonwebtoken

Related Vulnerability Description: 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).*

Matcher: javascript-matcher

*Package URL.** pkg:npm/jsonwebtoken@0.1.0

Mitigation

Upgrade to version: 4.2.2

References

Vulnerability Datasource: https://github.com/advisories/GHSA-c7hr-j4mj-j2w6

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2015-9235

Related Vulnerability URLs:

- https://auth0.com/blog/2015/03/31/critical-vulnerabilities-in-json-web-token-libraries/

- https://github.com/auth0/node-jsonwebtoken/commit/1bb584bc382295eeb7ee8c4452a673a77a68b687

- https://nodesecurity.io/advisories/17

- https://www.timmclean.net/2015/02/25/jwt-alg-none.html

- https://auth0.com/blog/2015/03/31/critical-vulnerabilities-in-json-web-token-libraries/

- https://github.com/auth0/node-jsonwebtoken/commit/1bb584bc382295eeb7ee8c4452a673a77a68b687

- https://nodesecurity.io/advisories/17

- https://www.timmclean.net/2015/02/25/jwt-alg-none.html

Finding 3 - GHSA-c7hr-j4mj-j2w6 in jsonwebtoken:0.4.0

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Critical (9.8)	41.15% / 97.31%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-c7hr-j4mj-j2w6', 'CVE-2015-9235']	28

Location

Component	Version
jsonwebtoken	0.4.0

File Path
/juice-shop/node_modules/jsonwebtoken/package.json

CVSS v3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: Verification Bypass in jsonwebtoken

Related Vulnerability Description: 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)*.

Matcher: javascript-matcher

*Package URL.** pkg:npm/jsonwebtoken@0.4.0

Mitigation

Upgrade to version: 4.2.2

References

Vulnerability Datasource: https://github.com/advisories/GHSA-c7hr-j4mj-j2w6

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2015-9235

Related Vulnerability URLs:

- https://auth0.com/blog/2015/03/31/critical-vulnerabilities-in-json-web-token-libraries/

- https://github.com/auth0/node-jsonwebtoken/commit/1bb584bc382295eeb7ee8c4452a673a77a68b687

- https://nodesecurity.io/advisories/17

- https://www.timmclean.net/2015/02/25/jwt-alg-none.html

- https://auth0.com/blog/2015/03/31/critical-vulnerabilities-in-json-web-token-libraries/

- https://github.com/auth0/node-jsonwebtoken/commit/1bb584bc382295eeb7ee8c4452a673a77a68b687

- https://nodesecurity.io/advisories/17

- https://www.timmclean.net/2015/02/25/jwt-alg-none.html

Finding 4 - GHSA-cchq-frgv-rjh5 in vm2:3.9.17

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Critical (9.8)	4.73% / 88.98%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-cchq-frgv-rjh5', 'CVE-2023-37466']	30

Location

Component	Version
vm2	3.9.17

File Path
/juice-shop/node_modules/vm2/package.json

CVSS v3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: vm2 Sandbox Escape vulnerability

Related Vulnerability Description: vm2 is an advanced vm/sandbox for Node.js. The library contains critical security issues and should not be used for production. The maintenance of the project has been discontinued. In vm2 for versions up to 3.9.19, Promise handler sanitization can be bypassed with the @@species accessor property allowing attackers to escape the sandbox and run arbitrary code, potentially allowing remote code execution inside the context of vm2 sandbox.

Matcher: javascript-matcher

Package URL: pkg:npm/vm2@3.9.17

References

Vulnerability Datasource: https://github.com/advisories/GHSA-cchq-frgv-rjh5

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2023-37466

Related Vulnerability URLs:

- https://github.com/patriksimek/vm2/security/advisories/GHSA-cchq-frgv-rjh5

- https://github.com/patriksimek/vm2/security/advisories/GHSA-cchq-frgv-rjh5

Finding 5 - GHSA-g644-9gfx-q4q4 in vm2:3.9.17

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Critical (9.8)	35.57% / 96.96%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-g644-9gfx-q4q4', 'CVE-2023-37903']	29

Location

Component	Version
vm2	3.9.17

File Path
/juice-shop/node_modules/vm2/package.json

CVSS v3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: vm2 Sandbox Escape vulnerability

Related Vulnerability Description: vm2 is an open source vm/sandbox for Node.js. In vm2 for versions up to and including 3.9.19, Node.js custom inspect function allows attackers to escape the sandbox and run arbitrary code. This may result in Remote Code Execution, assuming the attacker has arbitrary code execution primitive inside the context of vm2 sandbox. There are no patches and no known workarounds. Users are advised to find an alternative software.

Matcher: javascript-matcher

Package URL: pkg:npm/vm2@3.9.17

References

Vulnerability Datasource: https://github.com/advisories/GHSA-g644-9gfx-q4q4

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2023-37903

Related Vulnerability URLs:

- https://github.com/patriksimek/vm2/security/advisories/GHSA-g644-9gfx-q4q4

- https://security.netapp.com/advisory/ntap-20230831-0007/

- https://github.com/patriksimek/vm2/security/advisories/GHSA-g644-9gfx-q4q4

- https://security.netapp.com/advisory/ntap-20230831-0007/

Finding 6 - GHSA-jf85-cpcp-j695 in lodash:2.4.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Critical (9.1)	1.18% / 78.09%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-jf85-cpcp-j695', 'CVE-2019-10744']	34

Location

Component	Version
lodash	2.4.2

File Path
/juice-shop/node_modules/sanitize-html/node_modules/lodash/package.json

CVSS v3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: Prototype Pollution in lodash

Related Vulnerability Description: Versions of lodash lower than 4.17.12 are vulnerable to Prototype Pollution. The function defaultsDeep could be tricked into adding or modifying properties of Object.prototype using a constructor payload.

Matcher: javascript-matcher

Package URL: pkg:npm/lodash@2.4.2

Mitigation

Upgrade to version: 4.17.12

References

Vulnerability Datasource: https://github.com/advisories/GHSA-jf85-cpcp-j695

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2019-10744

Related Vulnerability URLs:

- https://access.redhat.com/errata/RHSA-2019:3024

- https://security.netapp.com/advisory/ntap-20191004-0005/

- https://snyk.io/vuln/SNYK-JS-LODASH-450202

- https://support.f5.com/csp/article/K47105354?utm_source=f5support&amp%3Butm_medium=RSS

- https://www.oracle.com/security-alerts/cpujan2021.html

- https://www.oracle.com/security-alerts/cpuoct2020.html

- https://access.redhat.com/errata/RHSA-2019:3024

- https://security.netapp.com/advisory/ntap-20191004-0005/

- https://snyk.io/vuln/SNYK-JS-LODASH-450202

- https://support.f5.com/csp/article/K47105354?utm_source=f5support&amp%3Butm_medium=RSS

- https://www.oracle.com/security-alerts/cpujan2021.html

- https://www.oracle.com/security-alerts/cpuoct2020.html

Finding 7 - GHSA-whpj-8f3w-67p5 in vm2:3.9.17

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Critical (9.8)	69.49% / 98.61%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-whpj-8f3w-67p5', 'CVE-2023-32314']	26

Location

Component	Version
vm2	3.9.17

File Path
/juice-shop/node_modules/vm2/package.json

CVSS v3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: vm2 Sandbox Escape vulnerability

Related Vulnerability Description: vm2 is a sandbox that can run untrusted code with Node's built-in modules. A sandbox escape vulnerability exists in vm2 for versions up to and including 3.9.17. It abuses an unexpected creation of a host object based on the specification of Proxy. As a result a threat actor can bypass the sandbox protections to gain remote code execution rights on the host running the sandbox. This vulnerability was patched in the release of version 3.9.18 of vm2. Users are advised to upgrade. There are no known workarounds for this vulnerability.

Matcher: javascript-matcher

Package URL: pkg:npm/vm2@3.9.17

Mitigation

Upgrade to version: 3.9.18

References

Vulnerability Datasource: https://github.com/advisories/GHSA-whpj-8f3w-67p5

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2023-32314

Related Vulnerability URLs:

- https://gist.github.com/arkark/e9f5cf5782dec8321095be3e52acf5ac

- https://github.com/patriksimek/vm2/commit/d88105f99752305c5b8a77b63ddee3ec86912daf

- https://github.com/patriksimek/vm2/releases/tag/3.9.18

- https://github.com/patriksimek/vm2/security/advisories/GHSA-whpj-8f3w-67p5

- https://gist.github.com/arkark/e9f5cf5782dec8321095be3e52acf5ac

- https://github.com/patriksimek/vm2/commit/d88105f99752305c5b8a77b63ddee3ec86912daf

- https://github.com/patriksimek/vm2/releases/tag/3.9.18

- https://github.com/patriksimek/vm2/security/advisories/GHSA-whpj-8f3w-67p5

Finding 8 - GHSA-xwcq-pm8m-c4vf in crypto-js:3.3.0

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Critical (9.1)	0.96% / 75.81%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-xwcq-pm8m-c4vf', 'CVE-2023-46233']	35

Location

Component	Version
crypto-js	3.3.0

File Path
/juice-shop/node_modules/crypto-js/package.json

CVSS v3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: crypto-js PBKDF2 1,000 times weaker than specified in 1993 and 1.3M times weaker than current standard

Related Vulnerability Description: crypto-js is a JavaScript library of crypto standards. Prior to version 4.2.0, crypto-js PBKDF2 is 1,000 times weaker than originally specified in 1993, and at least 1,300,000 times weaker than current industry standard. This is because it both defaults to SHA1, a cryptographic hash algorithm considered insecure since at least 2005, and defaults to one single iteration, a 'strength' or 'difficulty' value specified at 1,000 when specified in 1993. PBKDF2 relies on iteration count as a countermeasure to preimage and collision attacks. If used to protect passwords, the impact is high. If used to generate signatures, the impact is high. Version 4.2.0 contains a patch for this issue. As a workaround, configure crypto-js to use SHA256 with at least 250,000 iterations.

Matcher: javascript-matcher

Package URL: pkg:npm/crypto-js@3.3.0

Mitigation

Upgrade to version: 4.2.0

References

Vulnerability Datasource: https://github.com/advisories/GHSA-xwcq-pm8m-c4vf

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2023-46233

Related Vulnerability URLs:

- https://github.com/brix/crypto-js/commit/421dd538b2d34e7c24a5b72cc64dc2b9167db40a

- https://github.com/brix/crypto-js/security/advisories/GHSA-xwcq-pm8m-c4vf

- https://lists.debian.org/debian-lts-announce/2023/11/msg00025.html

- https://github.com/brix/crypto-js/commit/421dd538b2d34e7c24a5b72cc64dc2b9167db40a

- https://github.com/brix/crypto-js/security/advisories/GHSA-xwcq-pm8m-c4vf

- https://lists.debian.org/debian-lts-announce/2023/11/msg00025.html

High

Finding 9 - CVE-2025-4802 in libc6:2.36-9+deb12u10

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
High (7.8)	0.01% / 0.95%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['CVE-2025-4802']	80

Location

Component	Version
libc6	2.36-9+deb12u10

File Path
/var/lib/dpkg/status.d/libc6

CVSS v3

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Description

Vulnerability Namespace: debian:distro:debian:12

Vulnerability Description: Untrusted LD_LIBRARY_PATH environment variable vulnerability in the GNU C Library version 2.27 to 2.38 allows attacker controlled loading of dynamically shared library in statically compiled setuid binaries that call dlopen (including internal dlopen calls after setlocale or calls to NSS functions such as getaddrinfo).

Matcher: dpkg-matcher

Package URL: pkg:deb/debian/libc6@2.36-9%2Bdeb12u10?arch=arm64&distro=debian-12&upstream=glibc

Mitigation

Upgrade to version: 2.36-9+deb12u11

References

Vulnerability Datasource: https://security-tracker.debian.org/tracker/CVE-2025-4802

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2025-4802

Related Vulnerability URLs:

- https://sourceware.org/bugzilla/show_bug.cgi?id=32976

- https://sourceware.org/cgit/glibc/commit/?id=1e18586c5820e329f741d5c710275e165581380e

- http://www.openwall.com/lists/oss-security/2025/05/16/7

- http://www.openwall.com/lists/oss-security/2025/05/17/2

Finding 10 - CVE-2025-9230 in libssl3:3.0.17-1~deb12u2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
High (7.5)	0.02% / 4.67%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['CVE-2025-9230']	74

Location

Component	Version
libssl3	3.0.17-1~deb12u2

File Path
/var/lib/dpkg/status.d/libssl3

CVSS v3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description

Vulnerability Namespace: debian:distro:debian:12

Vulnerability Description: Issue summary: An application trying to decrypt CMS messages encrypted using password based encryption can trigger an out-of-bounds read and write. Impact summary: This out-of-bounds read may trigger a crash which leads to Denial of Service for an application. The out-of-bounds write can cause a memory corruption which can have various consequences including a Denial of Service or Execution of attacker-supplied code. Although the consequences of a successful exploit of this vulnerability could be severe, the probability that the attacker would be able to perform it is low. Besides, password based (PWRI) encryption support in CMS messages is very rarely used. For that reason the issue was assessed as Moderate severity according to our Security Policy. The FIPS modules in 3.5, 3.4, 3.3, 3.2, 3.1 and 3.0 are not affected by this issue, as the CMS implementation is outside the OpenSSL FIPS module boundary.

Related Vulnerability Description: Issue summary: An application trying to decrypt CMS messages encrypted using

password based encryption can trigger an out-of-bounds read and write.

Impact summary: This out-of-bounds read may trigger a crash which leads to

Denial of Service for an application. The out-of-bounds write can cause

a memory corruption which can have various consequences including

a Denial of Service or Execution of attacker-supplied code.

Although the consequences of a successful exploit of this vulnerability

could be severe, the probability that the attacker would be able to

perform it is low. Besides, password based (PWRI) encryption support in CMS

messages is very rarely used. For that reason the issue was assessed as

Moderate severity according to our Security Policy.

The FIPS modules in 3.5, 3.4, 3.3, 3.2, 3.1 and 3.0 are not affected by this

issue, as the CMS implementation is outside the OpenSSL FIPS module

boundary.

Matcher: dpkg-matcher

Package URL: pkg:deb/debian/libssl3@3.0.17-1~deb12u2?arch=arm64&distro=debian-12&upstream=openssl

Mitigation

Upgrade to version: 3.0.17-1~deb12u3

References

Vulnerability Datasource: https://security-tracker.debian.org/tracker/CVE-2025-9230

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2025-9230

Related Vulnerability URLs:

- https://github.com/openssl/openssl/commit/5965ea5dd6960f36d8b7f74f8eac67a8eb8f2b45

- https://github.com/openssl/openssl/commit/9e91358f365dee6c446dcdcdb01c04d2743fd280

- https://github.com/openssl/openssl/commit/a79c4ce559c6a3a8fd4109e9f33c1185d5bf2def

- https://github.com/openssl/openssl/commit/b5282d677551afda7d20e9c00e09561b547b2dfd

- https://github.com/openssl/openssl/commit/bae259a211ada6315dc50900686daaaaaa55f482

- https://github.openssl.org/openssl/extended-releases/commit/c2b96348bfa662f25f4fabf81958ae822063dae3

- https://github.openssl.org/openssl/extended-releases/commit/dfbaf161d8dafc1132dd88cd48ad990ed9b4c8ba

- https://openssl-library.org/news/secadv/20250930.txt

Finding 11 - GHSA-2p57-rm9w-gvfp in ip:2.0.1

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
High (8.1)	2.92% / 85.93%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-2p57-rm9w-gvfp', 'CVE-2024-29415']	31

Location

Component	Version
ip	2.0.1

File Path
/juice-shop/node_modules/ip/package.json

CVSS v3

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: ip SSRF improper categorization in isPublic

Related Vulnerability Description: The ip package through 2.0.1 for Node.js might allow SSRF because some IP addresses (such as 127.1, 01200034567, 012.1.2.3, 000:0:0000::01, and ::fFFf:127.0.0.1) are improperly categorized as globally routable via isPublic. NOTE: this issue exists because of an incomplete fix for CVE-2023-42282.

Matcher: javascript-matcher

Package URL: pkg:npm/ip@2.0.1

References

Vulnerability Datasource: https://github.com/advisories/GHSA-2p57-rm9w-gvfp

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2024-29415

Related Vulnerability URLs:

- https://github.com/indutny/node-ip/issues/150

- https://github.com/indutny/node-ip/pull/143

- https://github.com/indutny/node-ip/pull/144

- https://github.com/indutny/node-ip/issues/150

- https://github.com/indutny/node-ip/pull/143

- https://github.com/indutny/node-ip/pull/144

- https://security.netapp.com/advisory/ntap-20250117-0010/

Finding 12 - GHSA-35jh-r3h4-6jhm in lodash:2.4.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
High (7.2)	0.32% / 54.85%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-35jh-r3h4-6jhm', 'CVE-2021-23337']	42

Location

Component	Version
lodash	2.4.2

File Path
/juice-shop/node_modules/sanitize-html/node_modules/lodash/package.json

CVSS v3

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: Command Injection in lodash

Related Vulnerability Description: Lodash versions prior to 4.17.21 are vulnerable to Command Injection via the template function.

Matcher: javascript-matcher

Package URL: pkg:npm/lodash@2.4.2

Mitigation

Upgrade to version: 4.17.21

References

Vulnerability Datasource: https://github.com/advisories/GHSA-35jh-r3h4-6jhm

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2021-23337

Related Vulnerability URLs:

- https://cert-portal.siemens.com/productcert/pdf/ssa-637483.pdf

- https://github.com/lodash/lodash/blob/ddfd9b11a0126db2302cb70ec9973b66baec0975/lodash.js%23L14851

- https://security.netapp.com/advisory/ntap-20210312-0006/

- https://snyk.io/vuln/SNYK-JAVA-ORGFUJIONWEBJARS-1074932

- https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARS-1074930

- https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-1074928

- https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBLODASH-1074931

- https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1074929

- https://snyk.io/vuln/SNYK-JS-LODASH-1040724

- https://www.oracle.com//security-alerts/cpujul2021.html

- https://www.oracle.com/security-alerts/cpujan2022.html

- https://www.oracle.com/security-alerts/cpujul2022.html

- https://www.oracle.com/security-alerts/cpuoct2021.html

- https://cert-portal.siemens.com/productcert/pdf/ssa-637483.pdf

- https://github.com/lodash/lodash/blob/ddfd9b11a0126db2302cb70ec9973b66baec0975/lodash.js%23L14851

- https://security.netapp.com/advisory/ntap-20210312-0006/

- https://snyk.io/vuln/SNYK-JAVA-ORGFUJIONWEBJARS-1074932

- https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARS-1074930

- https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-1074928

- https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBLODASH-1074931

- https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1074929

- https://snyk.io/vuln/SNYK-JS-LODASH-1040724

- https://www.oracle.com//security-alerts/cpujul2021.html

- https://www.oracle.com/security-alerts/cpujan2022.html

- https://www.oracle.com/security-alerts/cpujul2022.html

- https://www.oracle.com/security-alerts/cpuoct2021.html

Finding 13 - GHSA-3h5v-q93c-6h6q in ws:7.4.6

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
High (7.5)	0.54% / 66.82%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-3h5v-q93c-6h6q', 'CVE-2024-37890']	40

Location

Component	Version
ws	7.4.6

File Path
/juice-shop/node_modules/engine.io/node_modules/ws/package.json

CVSS v3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: ws affected by a DoS when handling a request with many HTTP headers

Related Vulnerability Description: ws is an open source WebSocket client and server for Node.js. A request with a number of headers exceeding theserver.maxHeadersCount threshold could be used to crash a ws server. The vulnerability was fixed in ws@8.17.1 (e55e510) and backported to ws@7.5.10 (22c2876), ws@6.2.3 (eeb76d3), and ws@5.2.4 (4abd8f6). In vulnerable versions of ws, the issue can be mitigated in the following ways: 1. Reduce the maximum allowed length of the request headers using the --max-http-header-size=size and/or the maxHeaderSize options so that no more headers than the server.maxHeadersCount limit can be sent. 2. Set server.maxHeadersCount to 0 so that no limit is applied.

Matcher: javascript-matcher

Package URL: pkg:npm/ws@7.4.6

Mitigation

Upgrade to version: 7.5.10

References

Vulnerability Datasource: https://github.com/advisories/GHSA-3h5v-q93c-6h6q

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2024-37890

Related Vulnerability URLs:

- https://github.com/websockets/ws/commit/22c28763234aa75a7e1b76f5c01c181260d7917f

- https://github.com/websockets/ws/commit/4abd8f6de4b0b65ef80b3ff081989479ed93377e

- https://github.com/websockets/ws/commit/e55e5106f10fcbaac37cfa89759e4cc0d073a52c

- https://github.com/websockets/ws/commit/eeb76d313e2a00dd5247ca3597bba7877d064a63

- https://github.com/websockets/ws/issues/2230

- https://github.com/websockets/ws/pull/2231

- https://github.com/websockets/ws/security/advisories/GHSA-3h5v-q93c-6h6q

- https://nodejs.org/api/http.html#servermaxheaderscount

- https://github.com/websockets/ws/commit/22c28763234aa75a7e1b76f5c01c181260d7917f

- https://github.com/websockets/ws/commit/4abd8f6de4b0b65ef80b3ff081989479ed93377e

- https://github.com/websockets/ws/commit/e55e5106f10fcbaac37cfa89759e4cc0d073a52c

- https://github.com/websockets/ws/commit/eeb76d313e2a00dd5247ca3597bba7877d064a63

- https://github.com/websockets/ws/issues/2230

- https://github.com/websockets/ws/pull/2231

- https://github.com/websockets/ws/security/advisories/GHSA-3h5v-q93c-6h6q

- https://nodejs.org/api/http.html#servermaxheaderscount

Finding 14 - GHSA-446m-mv8f-q348 in moment:2.0.0

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
High (7.5)	0.24% / 47.74%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-446m-mv8f-q348', 'CVE-2017-18214']	43

Location

Component	Version
moment	2.0.0

File Path
/juice-shop/node_modules/express-jwt/node_modules/moment/package.json

CVSS v3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: Regular Expression Denial of Service in moment

Related Vulnerability Description: The moment module before 2.19.3 for Node.js is prone to a regular expression denial of service via a crafted date string, a different vulnerability than CVE-2016-4055.

Matcher: javascript-matcher

Package URL: pkg:npm/moment@2.0.0

Mitigation

Upgrade to version: 2.19.3

References

Vulnerability Datasource: https://github.com/advisories/GHSA-446m-mv8f-q348

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2017-18214

Related Vulnerability URLs:

- https://github.com/moment/moment/issues/4163

- https://nodesecurity.io/advisories/532

- https://www.tenable.com/security/tns-2019-02

- https://github.com/moment/moment/issues/4163

- https://nodesecurity.io/advisories/532

- https://www.tenable.com/security/tns-2019-02

Finding 15 - GHSA-44fp-w29j-9vj5 in multer:1.4.5-lts.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
High (7.5)	0.04% / 10.45%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-44fp-w29j-9vj5', 'CVE-2025-47935']	65

Location

Component	Version
multer	1.4.5-lts.2

File Path
/juice-shop/node_modules/multer/package.json

CVSS v3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: Multer vulnerable to Denial of Service via memory leaks from unclosed streams

Related Vulnerability Description: Multer is a node.js middleware for handling multipart/form-data. Versions prior to 2.0.0 are vulnerable to a resource exhaustion and memory leak issue due to improper stream handling. When the HTTP request stream emits an error, the internal busboy stream is not closed, violating Node.js stream safety guidance. This leads to unclosed streams accumulating over time, consuming memory and file descriptors. Under sustained or repeated failure conditions, this can result in denial of service, requiring manual server restarts to recover. All users of Multer handling file uploads are potentially impacted. Users should upgrade to 2.0.0 to receive a patch. No known workarounds are available.

Matcher: javascript-matcher

Package URL: pkg:npm/multer@1.4.5-lts.2

Mitigation

Upgrade to version: 2.0.0

References

Vulnerability Datasource: https://github.com/advisories/GHSA-44fp-w29j-9vj5

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2025-47935

Related Vulnerability URLs:

- https://github.com/expressjs/multer/commit/2c8505f207d923dd8de13a9f93a4563e59933665

- https://github.com/expressjs/multer/pull/1120

- https://github.com/expressjs/multer/security/advisories/GHSA-44fp-w29j-9vj5

Finding 16 - GHSA-4pg4-qvpc-4q3h in multer:1.4.5-lts.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
High (7.5)	0.04% / 10.45%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-4pg4-qvpc-4q3h', 'CVE-2025-47944']	66

Location

Component	Version
multer	1.4.5-lts.2

File Path
/juice-shop/node_modules/multer/package.json

CVSS v3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: Multer vulnerable to Denial of Service from maliciously crafted requests

Related Vulnerability Description: Multer is a node.js middleware for handling multipart/form-data. A vulnerability that is present starting in version 1.4.4-lts.1 and prior to version 2.0.0 allows an attacker to trigger a Denial of Service (DoS) by sending a

malformed multi-part upload request. This request causes an unhandled exception, leading to a crash of the process. Users should upgrade to version 2.0.0 to receive a patch. No known workarounds are available.

Matcher: javascript-matcher

Package URL: pkg:npm/multer@1.4.5-lts.2

Mitigation

Upgrade to version: 2.0.0

References

Vulnerability Datasource: https://github.com/advisories/GHSA-4pg4-qvpc-4q3h

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2025-47944

Related Vulnerability URLs:

- https://github.com/expressjs/multer/commit/2c8505f207d923dd8de13a9f93a4563e59933665

- https://github.com/expressjs/multer/issues/1176

- https://github.com/expressjs/multer/security/advisories/GHSA-4pg4-qvpc-4q3h

Finding 17 - GHSA-4xc9-xhrj-v574 in lodash:2.4.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
High (5.6)	0.21% / 43.29%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-4xc9-xhrj-v574', 'CVE-2018-16487']	46

Location

Component	Version
lodash	2.4.2

File Path
/juice-shop/node_modules/sanitize-html/node_modules/lodash/package.json

CVSS v3

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: Prototype Pollution in lodash

Related Vulnerability Description: A prototype pollution vulnerability was found in lodash <4.17.11 where the functions merge, mergeWith, and defaultsDeep can be tricked into adding or modifying properties of Object.prototype.

Matcher: javascript-matcher

Package URL: pkg:npm/lodash@2.4.2

Mitigation

Upgrade to version: 4.17.11

References

Vulnerability Datasource: https://github.com/advisories/GHSA-4xc9-xhrj-v574

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2018-16487

Related Vulnerability URLs:

- https://hackerone.com/reports/380873

- https://security.netapp.com/advisory/ntap-20190919-0004/

- https://hackerone.com/reports/380873

- https://security.netapp.com/advisory/ntap-20190919-0004/

Finding 18 - GHSA-6g6m-m6h5-w9gf in express-jwt:0.1.3

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
High (7.7)	0.10% / 27.57%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-6g6m-m6h5-w9gf', 'CVE-2020-15084']	56

Location

Component	Version
express-jwt	0.1.3

File Path
/juice-shop/node_modules/express-jwt/package.json

CVSS v3

CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:N

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: Authorization bypass in express-jwt

Related Vulnerability Description: 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.

Matcher: javascript-matcher

Package URL: pkg:npm/express-jwt@0.1.3

Mitigation

Upgrade to version: 6.0.0

References

Vulnerability Datasource: https://github.com/advisories/GHSA-6g6m-m6h5-w9gf

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2020-15084

Related Vulnerability URLs:

- https://github.com/auth0/express-jwt/commit/7ecab5f8f0cab5297c2b863596566eb0c019cdef

- https://github.com/auth0/express-jwt/security/advisories/GHSA-6g6m-m6h5-w9gf

- https://github.com/auth0/express-jwt/commit/7ecab5f8f0cab5297c2b863596566eb0c019cdef

- https://github.com/auth0/express-jwt/security/advisories/GHSA-6g6m-m6h5-w9gf

Finding 19 - GHSA-8cf7-32gw-wr33 in jsonwebtoken:0.1.0

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
High (8.1)	0.06% / 18.52%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-8cf7-32gw-wr33', 'CVE-2022-23539']	61

Location

Component	Version
jsonwebtoken	0.1.0

File Path
/juice-shop/node_modules/express-jwt/node_modules/jsonwebtoken/package.json

CVSS v3

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: jsonwebtoken unrestricted key type could lead to legacy keys usage

Related Vulnerability Description: Versions <=8.5.1 of jsonwebtoken library could be misconfigured so that legacy, insecure key types are used for signature verification. For example, DSA keys could be used with the RS256 algorithm. You are affected if you are using an algorithm and a key type other than a combination listed in the GitHub Security Advisory as unaffected. This issue has been fixed, please update to version 9.0.0. This version validates for asymmetric key type and algorithm combinations. Please refer to the above mentioned algorithm / key type combinations for the valid secure configuration. After updating to version 9.0.0, if you still intend to continue with signing or verifying tokens using invalid key type/algorithm value combinations, you'll need to set the allowInvalidAsymmetricKeyTypes option to true in the sign() and/or verify() functions.

Matcher: javascript-matcher

Package URL: pkg:npm/jsonwebtoken@0.1.0

Mitigation

Upgrade to version: 9.0.0

References

Vulnerability Datasource: https://github.com/advisories/GHSA-8cf7-32gw-wr33

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2022-23539

Related Vulnerability URLs:

- https://github.com/auth0/node-jsonwebtoken/commit/e1fa9dcc12054a8681db4e6373da1b30cf7016e3

- https://github.com/auth0/node-jsonwebtoken/security/advisories/GHSA-8cf7-32gw-wr33

- https://security.netapp.com/advisory/ntap-20240621-0007/

- https://github.com/auth0/node-jsonwebtoken/commit/e1fa9dcc12054a8681db4e6373da1b30cf7016e3

- https://github.com/auth0/node-jsonwebtoken/security/advisories/GHSA-8cf7-32gw-wr33

- https://security.netapp.com/advisory/ntap-20240621-0007/

Finding 20 - GHSA-8cf7-32gw-wr33 in jsonwebtoken:0.4.0

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
High (8.1)	0.06% / 18.52%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-8cf7-32gw-wr33', 'CVE-2022-23539']	62

Location

Component	Version
jsonwebtoken	0.4.0

File Path
/juice-shop/node_modules/jsonwebtoken/package.json

CVSS v3

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: jsonwebtoken unrestricted key type could lead to legacy keys usage

Related Vulnerability Description: Versions <=8.5.1 of jsonwebtoken library could be misconfigured so that legacy, insecure key types are used for signature verification. For example, DSA keys could be used with the RS256 algorithm. You are affected if you are using an algorithm and a key type other than a combination listed in the GitHub Security Advisory as unaffected. This issue has been fixed, please update to version 9.0.0. This version validates for asymmetric key type and algorithm combinations. Please refer to the above mentioned algorithm / key type combinations for the valid secure configuration. After updating to version 9.0.0, if you still intend to continue with signing or verifying tokens using invalid key type/algorithm value combinations, you'll need to set the allowInvalidAsymmetricKeyTypes option to true in the sign() and/or verify() functions.

Matcher: javascript-matcher

Package URL: pkg:npm/jsonwebtoken@0.4.0

Mitigation

Upgrade to version: 9.0.0

References

Vulnerability Datasource: https://github.com/advisories/GHSA-8cf7-32gw-wr33

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2022-23539

Related Vulnerability URLs:

- https://github.com/auth0/node-jsonwebtoken/commit/e1fa9dcc12054a8681db4e6373da1b30cf7016e3

- https://github.com/auth0/node-jsonwebtoken/security/advisories/GHSA-8cf7-32gw-wr33

- https://security.netapp.com/advisory/ntap-20240621-0007/

- https://github.com/auth0/node-jsonwebtoken/commit/e1fa9dcc12054a8681db4e6373da1b30cf7016e3

- https://github.com/auth0/node-jsonwebtoken/security/advisories/GHSA-8cf7-32gw-wr33

- https://security.netapp.com/advisory/ntap-20240621-0007/

Finding 21 - GHSA-8hfj-j24r-96c4 in moment:2.0.0

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
High (7.5)	0.69% / 71.13%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-8hfj-j24r-96c4', 'CVE-2022-24785']	38

Location

Component	Version
moment	2.0.0

File Path
/juice-shop/node_modules/express-jwt/node_modules/moment/package.json

CVSS v3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: Path Traversal: 'dir/../../filename' in moment.locale

Related Vulnerability Description: Moment.js is a JavaScript date library for parsing, validating, manipulating, and formatting dates. A path traversal vulnerability impacts npm (server) users of Moment.js between versions 1.0.1 and 2.29.1, especially if a user-provided locale string is directly used to switch moment locale. This problem is patched in 2.29.2, and the patch can be applied to all affected versions. As a workaround, sanitize the user-provided locale name before passing it to Moment.js.

Matcher: javascript-matcher

Package URL: pkg:npm/moment@2.0.0

Mitigation

Upgrade to version: 2.29.2

References

Vulnerability Datasource: https://github.com/advisories/GHSA-8hfj-j24r-96c4

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2022-24785

Related Vulnerability URLs:

- https://github.com/moment/moment/commit/4211bfc8f15746be4019bba557e29a7ba83d54c5

- https://github.com/moment/moment/security/advisories/GHSA-8hfj-j24r-96c4

- https://lists.debian.org/debian-lts-announce/2023/01/msg00035.html

- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/6QIO6YNLTK2T7SPKDS4JEL45FANLNC2Q/

- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/ORJX2LF6KMPIHP6B2P6KZIVKMLE3LVJ5/

- https://security.netapp.com/advisory/ntap-20220513-0006/

- https://www.tenable.com/security/tns-2022-09

- https://github.com/moment/moment/commit/4211bfc8f15746be4019bba557e29a7ba83d54c5

- https://github.com/moment/moment/security/advisories/GHSA-8hfj-j24r-96c4

- https://lists.debian.org/debian-lts-announce/2023/01/msg00035.html

- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/6QIO6YNLTK2T7SPKDS4JEL45FANLNC2Q/

- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/ORJX2LF6KMPIHP6B2P6KZIVKMLE3LVJ5/

- https://security.netapp.com/advisory/ntap-20220513-0006/

- https://www.tenable.com/security/tns-2022-09

Finding 22 - GHSA-cgfm-xwp7-2cvr in sanitize-html:1.4.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
High (7.5)	0.06% / 17.71%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-cgfm-xwp7-2cvr', 'CVE-2022-25887']	63

Location

Component	Version
sanitize-html	1.4.2

File Path
/juice-shop/node_modules/sanitize-html/package.json

CVSS v3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: Sanitize-html Vulnerable To REDoS Attacks

Related Vulnerability Description: The package sanitize-html before 2.7.1 are vulnerable to Regular Expression Denial of Service (ReDoS) due to insecure global regular expression replacement logic of HTML comment removal.

Matcher: javascript-matcher

Package URL: pkg:npm/sanitize-html@1.4.2

Mitigation

Upgrade to version: 2.7.1

References

Vulnerability Datasource: https://github.com/advisories/GHSA-cgfm-xwp7-2cvr

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2022-25887

Related Vulnerability URLs:

- https://github.com/apostrophecms/sanitize-html/commit/b4682c12fd30e12e82fa2d9b766de91d7d2cd23c

- https://github.com/apostrophecms/sanitize-html/pull/557

- https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-3008102

- https://security.snyk.io/vuln/SNYK-JS-SANITIZEHTML-2957526

- https://github.com/apostrophecms/sanitize-html/commit/b4682c12fd30e12e82fa2d9b766de91d7d2cd23c

- https://github.com/apostrophecms/sanitize-html/pull/557

- https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-3008102

- https://security.snyk.io/vuln/SNYK-JS-SANITIZEHTML-2957526

Finding 23 - GHSA-fjgf-rc76-4x9p in multer:1.4.5-lts.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
High (7.5)	0.02% / 3.38%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-fjgf-rc76-4x9p', 'CVE-2025-7338']	76

Location

Component	Version
multer	1.4.5-lts.2

File Path
/juice-shop/node_modules/multer/package.json

CVSS v3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: Multer vulnerable to Denial of Service via unhandled exception from malformed request

Related Vulnerability Description: Multer is a node.js middleware for handling multipart/form-data. A vulnerability that is present starting in version 1.4.4-lts.1 and prior to version 2.0.2 allows an attacker to trigger a Denial of Service (DoS) by sending a malformed multi-part upload request. This request causes an unhandled exception, leading to a crash of the process. Users should upgrade to version 2.0.2 to receive a patch. No known workarounds are available.

Matcher: javascript-matcher

Package URL: pkg:npm/multer@1.4.5-lts.2

Mitigation

Upgrade to version: 2.0.2

References

Vulnerability Datasource: https://github.com/advisories/GHSA-fjgf-rc76-4x9p

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2025-7338

Related Vulnerability URLs:

- https://cna.openjsf.org/security-advisories.html

- https://github.com/expressjs/multer/commit/adfeaf669f0e7fe953eab191a762164a452d143b

- https://github.com/expressjs/multer/security/advisories/GHSA-fjgf-rc76-4x9p

Finding 24 - GHSA-g5hg-p3ph-g8qg in multer:1.4.5-lts.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
High	0.06% / 20.07%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-g5hg-p3ph-g8qg', 'CVE-2025-48997']	60

Location

Component	Version
multer	1.4.5-lts.2

File Path
/juice-shop/node_modules/multer/package.json

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: Multer vulnerable to Denial of Service via unhandled exception

Related Vulnerability Description: Multer is a node.js middleware for handling multipart/form-data. A vulnerability that is present starting in version 1.4.4-lts.1 and prior to version 2.0.1 allows an attacker to trigger a Denial of Service (DoS) by sending an upload file request with an empty string field name. This request causes an unhandled exception, leading to a crash of the process. Users should upgrade to 2.0.1 to receive a patch. No known workarounds are available.

Matcher: javascript-matcher

Package URL: pkg:npm/multer@1.4.5-lts.2

Mitigation

Upgrade to version: 2.0.1

References

Vulnerability Datasource: https://github.com/advisories/GHSA-g5hg-p3ph-g8qg

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2025-48997

Related Vulnerability URLs:

- https://github.com/expressjs/multer/commit/35a3272b611945155e046dd5cef11088587635e9

- https://github.com/expressjs/multer/issues/1233

- https://github.com/expressjs/multer/pull/1256

- https://github.com/expressjs/multer/security/advisories/GHSA-g5hg-p3ph-g8qg

Finding 25 - GHSA-gjcw-v447-2w7q in jws:0.2.6

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
High (8.7)	N.A. / N.A.	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-gjcw-v447-2w7q', 'CVE-2016-1000223']	89

Location

Component	Version
jws	0.2.6

File Path
/juice-shop/node_modules/jws/package.json

CVSS v3

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:N

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: Forgeable Public/Private Tokens in jws

Matcher: javascript-matcher

Package URL: pkg:npm/jws@0.2.6

Mitigation

Upgrade to version: 3.0.0

References

Vulnerability Datasource: https://github.com/advisories/GHSA-gjcw-v447-2w7q

Related Vulnerability Datasource: nvd

Finding 26 - GHSA-grv7-fg5c-xmjg in braces:2.3.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
High (7.5)	0.16% / 37.54%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-grv7-fg5c-xmjg', 'CVE-2024-4068']	50

Location

Component	Version
braces	2.3.2

File Path
/juice-shop/node_modules/braces/package.json

CVSS v3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: Uncontrolled resource consumption in braces

Related Vulnerability Description: The NPM package braces, versions prior to 3.0.3, fails to limit the number of characters it can handle, which could lead to Memory Exhaustion. In lib/parse.js, if a malicious user sends "imbalanced braces" as input, the parsing will enter a loop, which will cause the program to start allocating heap memory without freeing it at any moment of the loop. Eventually, the JavaScript heap limit is reached, and the program will crash.

Matcher: javascript-matcher

Package URL: pkg:npm/braces@2.3.2

Mitigation

Upgrade to version: 3.0.3

References

Vulnerability Datasource: https://github.com/advisories/GHSA-grv7-fg5c-xmjg

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2024-4068

Related Vulnerability URLs:

- https://devhub.checkmarx.com/cve-details/CVE-2024-4068/

- https://github.com/micromatch/braces/commit/415d660c3002d1ab7e63dbf490c9851da80596ff

- https://github.com/micromatch/braces/issues/35

- https://github.com/micromatch/braces/pull/37

- https://github.com/micromatch/braces/pull/40

- https://devhub.checkmarx.com/cve-details/CVE-2024-4068/

- https://github.com/micromatch/braces/commit/415d660c3002d1ab7e63dbf490c9851da80596ff

- https://github.com/micromatch/braces/issues/35

- https://github.com/micromatch/braces/pull/37

- https://github.com/micromatch/braces/pull/40

Finding 27 - GHSA-p6mc-m468-83gw in lodash.set:4.3.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
High (7.4)	2.00% / 83.05%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-p6mc-m468-83gw', 'CVE-2020-8203']	33

Location

Component	Version
lodash.set	4.3.2

File Path
/juice-shop/node_modules/lodash.set/package.json

CVSS v3

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:H

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: Prototype Pollution in lodash

Related Vulnerability Description: Prototype pollution attack when using _.zipObjectDeep in lodash before 4.17.20.

Matcher: javascript-matcher

Package URL: pkg:npm/lodash.set@4.3.2

References

Vulnerability Datasource: https://github.com/advisories/GHSA-p6mc-m468-83gw

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2020-8203

Related Vulnerability URLs:

- https://github.com/lodash/lodash/issues/4874

- https://hackerone.com/reports/712065

- https://security.netapp.com/advisory/ntap-20200724-0006/

- https://www.oracle.com//security-alerts/cpujul2021.html

- https://www.oracle.com/security-alerts/cpuApr2021.html

- https://www.oracle.com/security-alerts/cpuapr2022.html

- https://www.oracle.com/security-alerts/cpujan2022.html

- https://www.oracle.com/security-alerts/cpuoct2021.html

- https://github.com/lodash/lodash/issues/4874

- https://hackerone.com/reports/712065

- https://security.netapp.com/advisory/ntap-20200724-0006/

- https://www.oracle.com//security-alerts/cpujul2021.html

- https://www.oracle.com/security-alerts/cpuApr2021.html

- https://www.oracle.com/security-alerts/cpuapr2022.html

- https://www.oracle.com/security-alerts/cpujan2022.html

- https://www.oracle.com/security-alerts/cpuoct2021.html

Finding 28 - GHSA-rc47-6667-2j5j in http-cache-semantics:3.8.1

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
High (7.5)	0.16% / 37.49%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-rc47-6667-2j5j', 'CVE-2022-25881']	51

Location

Component	Version
http-cache-semantics	3.8.1

File Path
/juice-shop/node_modules/http-cache-semantics/package.json

CVSS v3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: http-cache-semantics vulnerable to Regular Expression Denial of Service

Related Vulnerability Description: This affects versions of the package http-cache-semantics before 4.1.1. The issue can be exploited via malicious request header values sent to a server, when that server reads the cache policy from the request using this library.

Matcher: javascript-matcher

Package URL: pkg:npm/http-cache-semantics@3.8.1

Mitigation

Upgrade to version: 4.1.1

References

Vulnerability Datasource: https://github.com/advisories/GHSA-rc47-6667-2j5j

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2022-25881

Related Vulnerability URLs:

- https://github.com/kornelski/http-cache-semantics/blob/master/index.js%23L83

- https://security.netapp.com/advisory/ntap-20230622-0008/

- https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-3253332

- https://security.snyk.io/vuln/SNYK-JS-HTTPCACHESEMANTICS-3248783

- https://github.com/kornelski/http-cache-semantics/blob/master/index.js%23L83

- https://security.netapp.com/advisory/ntap-20230622-0008/

- https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-3253332

- https://security.snyk.io/vuln/SNYK-JS-HTTPCACHESEMANTICS-3248783

Finding 29 - GHSA-vj76-c3g6-qr5v in tar-fs:2.1.3

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
High	0.07% / 20.90%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-vj76-c3g6-qr5v', 'CVE-2025-59343']	59

Location

Component	Version
tar-fs	2.1.3

File Path
/juice-shop/node_modules/tar-fs/package.json

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: tar-fs has a symlink validation bypass if destination directory is predictable with a specific tarball

Related Vulnerability Description: tar-fs provides filesystem bindings for tar-stream. Versions prior to 3.1.1, 2.1.3, and 1.16.5 are vulnerable to symlink validation bypass if the destination directory is predictable with a specific tarball. This issue has been patched in version 3.1.1, 2.1.4, and 1.16.6. A workaround involves using the ignore option on non files/directories.

Matcher: javascript-matcher

Package URL: pkg:npm/tar-fs@2.1.3

Mitigation

Upgrade to version: 2.1.4

References

Vulnerability Datasource: https://github.com/advisories/GHSA-vj76-c3g6-qr5v

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2025-59343

Related Vulnerability URLs:

- https://github.com/mafintosh/tar-fs/commit/0bd54cdf06da2b7b5b95cd4b062c9f4e0a8c4e09

- https://github.com/mafintosh/tar-fs/security/advisories/GHSA-vj76-c3g6-qr5v

Finding 30 - javascript.lang.security.audit.code-string-concat.code-string-concat

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
High	N.A. / N.A.	Active	Nov. 12, 2025	0 days	Admin User (admin)	95	18

Location

Line Number
62

File Path
/src/routes/userProfile.ts

Description

Result message: Found data from an Express or Next web request flowing to eval. If this data is user-controllable this can lead to execution of arbitrary system commands in the context of your application process. Avoid eval whenever possible.

References

https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference/Global_Objects/eval

https://nodejs.org/api/child_process.html#child_processexeccommand-options-callback

https://www.stackhawk.com/blog/nodejs-command-injection-examples-and-prevention/

https://ckarande.gitbooks.io/owasp-nodegoat-tutorial/content/tutorial/a1_-_server_side_js_injection.html

Finding 31 - javascript.sequelize.security.audit.sequelize-injection-express.express-sequelize-injection

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
High	N.A. / N.A.	Active	Nov. 12, 2025	0 days	Admin User (admin)	89	17

Location

Line Number
23

File Path
/src/routes/search.ts

Description

Result message: Detected a sequelize statement that is tainted by user-input. This could lead to SQL injection if the variable is user-controlled and is not properly sanitized. In order to prevent SQL injection, it is recommended to use parameterized queries or prepared statements.

References

https://sequelize.org/docs/v6/core-concepts/raw-queries/#replacements

Finding 32 - javascript.sequelize.security.audit.sequelize-injection-express.express-sequelize-injection

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
High	N.A. / N.A.	Active	Nov. 12, 2025	0 days	Admin User (admin)	89	1

Location

Line Number
5

File Path
/src/data/static/codefixes/dbSchemaChallenge_1.ts

Description

Result message: Detected a sequelize statement that is tainted by user-input. This could lead to SQL injection if the variable is user-controlled and is not properly sanitized. In order to prevent SQL injection, it is recommended to use parameterized queries or prepared statements.

References

https://sequelize.org/docs/v6/core-concepts/raw-queries/#replacements

Finding 33 - javascript.sequelize.security.audit.sequelize-injection-express.express-sequelize-injection

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
High	N.A. / N.A.	Active	Nov. 12, 2025	0 days	Admin User (admin)	89	4

Location

Line Number
10

File Path
/src/data/static/codefixes/unionSqlInjectionChallenge_3.ts

Description

Result message: Detected a sequelize statement that is tainted by user-input. This could lead to SQL injection if the variable is user-controlled and is not properly sanitized. In order to prevent SQL injection, it is recommended to use parameterized queries or prepared statements.

References

https://sequelize.org/docs/v6/core-concepts/raw-queries/#replacements

Finding 34 - javascript.sequelize.security.audit.sequelize-injection-express.express-sequelize-injection

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
High	N.A. / N.A.	Active	Nov. 12, 2025	0 days	Admin User (admin)	89	3

Location

Line Number
6

File Path
/src/data/static/codefixes/unionSqlInjectionChallenge_1.ts

Description

Result message: Detected a sequelize statement that is tainted by user-input. This could lead to SQL injection if the variable is user-controlled and is not properly sanitized. In order to prevent SQL injection, it is recommended to use parameterized queries or prepared statements.

References

https://sequelize.org/docs/v6/core-concepts/raw-queries/#replacements

Finding 35 - javascript.sequelize.security.audit.sequelize-injection-express.express-sequelize-injection

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
High	N.A. / N.A.	Active	Nov. 12, 2025	0 days	Admin User (admin)	89	2

Location

Line Number
11

File Path
/src/data/static/codefixes/dbSchemaChallenge_3.ts

Description

Result message: Detected a sequelize statement that is tainted by user-input. This could lead to SQL injection if the variable is user-controlled and is not properly sanitized. In order to prevent SQL injection, it is recommended to use parameterized queries or prepared statements.

References

https://sequelize.org/docs/v6/core-concepts/raw-queries/#replacements

Finding 36 - javascript.sequelize.security.audit.sequelize-injection-express.express-sequelize-injection

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
High	N.A. / N.A.	Active	Nov. 12, 2025	0 days	Admin User (admin)	89	13

Location

Line Number
34

File Path
/src/routes/login.ts

Description

Result message: Detected a sequelize statement that is tainted by user-input. This could lead to SQL injection if the variable is user-controlled and is not properly sanitized. In order to prevent SQL injection, it is recommended to use parameterized queries or prepared statements.

References

https://sequelize.org/docs/v6/core-concepts/raw-queries/#replacements

Medium

Finding 37 - CVE-2025-8058 in libc6:2.36-9+deb12u10

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Medium	0.01% / 0.74%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['CVE-2025-8058']	82

Location

Component	Version
libc6	2.36-9+deb12u10

File Path
/var/lib/dpkg/status.d/libc6

Description

Vulnerability Namespace: debian:distro:debian:12

Vulnerability Description: The regcomp function in the GNU C library version from 2.4 to 2.41 is subject to a double free if some previous allocation fails. It can be accomplished either by a malloc failure or by using an interposed malloc that injects random malloc failures. The double free can allow buffer manipulation depending of how the regex is constructed. This issue affects all architectures and ABIs supported by the GNU C library.

Related Vulnerability Description: The regcomp function in the GNU C library version from 2.4 to 2.41 is

subject to a double free if some previous allocation fails. It can be

accomplished either by a malloc failure or by using an interposed malloc

that injects random malloc failures. The double free can allow buffer

manipulation depending of how the regex is constructed. This issue

affects all architectures and ABIs supported by the GNU C library.

Matcher: dpkg-matcher

Package URL: pkg:deb/debian/libc6@2.36-9%2Bdeb12u10?arch=arm64&distro=debian-12&upstream=glibc

Mitigation

Upgrade to version: 2.36-9+deb12u13

References

Vulnerability Datasource: https://security-tracker.debian.org/tracker/CVE-2025-8058

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2025-8058

Related Vulnerability URLs:

- https://sourceware.org/bugzilla/show_bug.cgi?id=33185

- https://sourceware.org/git/?p=glibc.git;a=commit;h=3ff17af18c38727b88d9115e536c069e6b5d601f

Finding 38 - CVE-2025-9232 in libssl3:3.0.17-1~deb12u2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Medium (5.9)	0.03% / 6.61%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['CVE-2025-9232']	75

Location

Component	Version
libssl3	3.0.17-1~deb12u2

File Path
/var/lib/dpkg/status.d/libssl3

CVSS v3

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

Description

Vulnerability Namespace: debian:distro:debian:12

Vulnerability Description: Issue summary: An application using the OpenSSL HTTP client API functions may trigger an out-of-bounds read if the 'no_proxy' environment variable is set and the host portion of the authority component of the HTTP URL is an IPv6 address. Impact summary: An out-of-bounds read can trigger a crash which leads to Denial of Service for an application. The OpenSSL HTTP client API functions can be used directly by applications but they are also used by the OCSP client functions and CMP (Certificate Management Protocol) client implementation in OpenSSL. However the URLs used by these implementations are unlikely to be controlled by an attacker. In this vulnerable code the out of bounds read can only trigger a crash. Furthermore the vulnerability requires an attacker-controlled URL to be passed from an application to the OpenSSL function and the user has to have a 'no_proxy' environment variable set. For the aforementioned reasons the issue was assessed as Low severity. The vulnerable code was introduced in the following patch releases: 3.0.16, 3.1.8, 3.2.4, 3.3.3, 3.4.0 and 3.5.0. The FIPS modules in 3.5, 3.4, 3.3, 3.2, 3.1 and 3.0 are not affected by this issue, as the HTTP client implementation is outside the OpenSSL FIPS module boundary.

Related Vulnerability Description: Issue summary: An application using the OpenSSL HTTP client API functions may

trigger an out-of-bounds read if the 'no_proxy' environment variable is set and

the host portion of the authority component of the HTTP URL is an IPv6 address.

Impact summary: An out-of-bounds read can trigger a crash which leads to

Denial of Service for an application.

The OpenSSL HTTP client API functions can be used directly by applications

but they are also used by the OCSP client functions and CMP (Certificate

Management Protocol) client implementation in OpenSSL. However the URLs used

by these implementations are unlikely to be controlled by an attacker.

In this vulnerable code the out of bounds read can only trigger a crash.

Furthermore the vulnerability requires an attacker-controlled URL to be

passed from an application to the OpenSSL function and the user has to have

a 'no_proxy' environment variable set. For the aforementioned reasons the

issue was assessed as Low severity.

The vulnerable code was introduced in the following patch releases:

3.0.16, 3.1.8, 3.2.4, 3.3.3, 3.4.0 and 3.5.0.

The FIPS modules in 3.5, 3.4, 3.3, 3.2, 3.1 and 3.0 are not affected by this

issue, as the HTTP client implementation is outside the OpenSSL FIPS module

boundary.

Matcher: dpkg-matcher

Package URL: pkg:deb/debian/libssl3@3.0.17-1~deb12u2?arch=arm64&distro=debian-12&upstream=openssl

Mitigation

Upgrade to version: 3.0.17-1~deb12u3

References

Vulnerability Datasource: https://security-tracker.debian.org/tracker/CVE-2025-9232

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2025-9232

Related Vulnerability URLs:

- https://github.com/openssl/openssl/commit/2b4ec20e47959170422922eaff25346d362dcb35

- https://github.com/openssl/openssl/commit/654dc11d23468a74fc8ea4672b702dd3feb7be4b

- https://github.com/openssl/openssl/commit/7cf21a30513c9e43c4bc3836c237cf086e194af3

- https://github.com/openssl/openssl/commit/89e790ac431125a4849992858490bed6b225eadf

- https://github.com/openssl/openssl/commit/bbf38c034cdabd0a13330abcc4855c866f53d2e0

- https://openssl-library.org/news/secadv/20250930.txt

Finding 39 - GHSA-25hc-qcg6-38wj in socket.io:3.1.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Medium (7.3)	0.10% / 28.48%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-25hc-qcg6-38wj', 'CVE-2024-38355']	57

Location

Component	Version
socket.io	3.1.2

File Path
/juice-shop/node_modules/socket.io/package.json

CVSS v3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: socket.io has an unhandled 'error' event

Related Vulnerability Description: Socket.IO is an open source, real-time, bidirectional, event-based, communication framework. A specially crafted Socket.IO packet can trigger an uncaught exception on the Socket.IO server, thus killing the Node.js process. This issue is fixed by commit 15af22fc22 which has been included in socket.io@4.6.2 (released in May 2023). The fix was backported in the 2.x branch as well with commit d30630ba10. Users are advised to upgrade. Users unable to upgrade may attach a listener for the "error" event to catch these errors.

Matcher: javascript-matcher

Package URL: pkg:npm/socket.io@3.1.2

Mitigation

Upgrade to version: 4.6.2

References

Vulnerability Datasource: https://github.com/advisories/GHSA-25hc-qcg6-38wj

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2024-38355

Related Vulnerability URLs:

- https://github.com/socketio/socket.io/commit/15af22fc22bc6030fcead322c106f07640336115

- https://github.com/socketio/socket.io/commit/d30630ba10562bf987f4d2b42440fc41a828119c

- https://github.com/socketio/socket.io/security/advisories/GHSA-25hc-qcg6-38wj

- https://github.com/socketio/socket.io/commit/15af22fc22bc6030fcead322c106f07640336115

- https://github.com/socketio/socket.io/commit/d30630ba10562bf987f4d2b42440fc41a828119c

- https://github.com/socketio/socket.io/security/advisories/GHSA-25hc-qcg6-38wj

- https://www.vicarius.io/vsociety/posts/unhandled-exception-in-socketio-cve-2024-38355

Finding 40 - GHSA-3j7m-hmh3-9jmp in sanitize-html:1.4.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Medium (6.1)	0.33% / 55.34%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-3j7m-hmh3-9jmp', 'CVE-2016-1000237']	44

Location

Component	Version
sanitize-html	1.4.2

File Path
/juice-shop/node_modules/sanitize-html/package.json

CVSS v3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: Cross-Site Scripting in sanitize-html

Related Vulnerability Description: sanitize-html before 1.4.3 has XSS.

Matcher: javascript-matcher

Package URL: pkg:npm/sanitize-html@1.4.2

Mitigation

Upgrade to version: 1.4.3

References

Vulnerability Datasource: https://github.com/advisories/GHSA-3j7m-hmh3-9jmp

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2016-1000237

Related Vulnerability URLs:

- https://nodesecurity.io/advisories/135

- https://raw.githubusercontent.com/distributedweaknessfiling/cvelist/master/2016/1000xxx/CVE-2016-1000237.json

- https://nodesecurity.io/advisories/135

- https://raw.githubusercontent.com/distributedweaknessfiling/cvelist/master/2016/1000xxx/CVE-2016-1000237.json

Finding 41 - GHSA-87vv-r9j6-g5qv in moment:2.0.0

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Medium (6.5)	1.35% / 79.52%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-87vv-r9j6-g5qv', 'CVE-2016-4055']	36

Location

Component	Version
moment	2.0.0

File Path
/juice-shop/node_modules/express-jwt/node_modules/moment/package.json

CVSS v3

CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: Regular Expression Denial of Service in moment

Related Vulnerability Description: The duration function in the moment package before 2.11.2 for Node.js allows remote attackers to cause a denial of service (CPU consumption) via a long string, aka a "regular expression Denial of Service (ReDoS)."

Matcher: javascript-matcher

Package URL: pkg:npm/moment@2.0.0

Mitigation

Upgrade to version: 2.11.2

References

Vulnerability Datasource: https://github.com/advisories/GHSA-87vv-r9j6-g5qv

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2016-4055

Related Vulnerability URLs:

- http://www.openwall.com/lists/oss-security/2016/04/20/11

- http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html

- http://www.securityfocus.com/bid/95849

- https://lists.apache.org/thread.html/10f0f3aefd51444d1198c65f44ffdf2d78ca3359423dbc1c168c9731%40%3Cdev.flink.apache.org%3E

- https://lists.apache.org/thread.html/17ff53f7999e74fbe3cc0ceb4e1c3b00b180b7c5afec8e978837bc49%40%3Cuser.flink.apache.org%3E

-

https://lists.apache.org/thread.html/52bafac05ad174000ea465fe275fd3cc7bd5c25535a7631c0bc9bfb2%40%3Cuser.flink.apache.org%3E

- https://lists.apache.org/thread.html/54df3aeb4239b64b50b356f0ca6f986e3c4ca5b84c515dce077c7854%40%3Cuser.flink.apache.org%3E

- https://nodesecurity.io/advisories/55

- https://www.tenable.com/security/tns-2019-02

- http://www.openwall.com/lists/oss-security/2016/04/20/11

- http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html

- http://www.securityfocus.com/bid/95849

- https://lists.apache.org/thread.html/10f0f3aefd51444d1198c65f44ffdf2d78ca3359423dbc1c168c9731%40%3Cdev.flink.apache.org%3E

- https://lists.apache.org/thread.html/17ff53f7999e74fbe3cc0ceb4e1c3b00b180b7c5afec8e978837bc49%40%3Cuser.flink.apache.org%3E

- https://lists.apache.org/thread.html/52bafac05ad174000ea465fe275fd3cc7bd5c25535a7631c0bc9bfb2%40%3Cuser.flink.apache.org%3E

- https://lists.apache.org/thread.html/54df3aeb4239b64b50b356f0ca6f986e3c4ca5b84c515dce077c7854%40%3Cuser.flink.apache.org%3E

- https://nodesecurity.io/advisories/55

- https://www.tenable.com/security/tns-2019-02

Finding 42 - GHSA-8g4m-cjm2-96wq in notevil:1.3.3

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Medium (6.5)	0.30% / 53.36%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-8g4m-cjm2-96wq', 'CVE-2021-23771']	45

Location

Component	Version
notevil	1.3.3

File Path
/juice-shop/node_modules/notevil/package.json

CVSS v3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: Sandbox escape in notevil and argencoders-notevil

Related Vulnerability Description: 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.

Matcher: javascript-matcher

Package URL: pkg:npm/notevil@1.3.3

References

Vulnerability Datasource: https://github.com/advisories/GHSA-8g4m-cjm2-96wq

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2021-23771

Related Vulnerability URLs:

- https://snyk.io/vuln/SNYK-JS-ARGENCODERSNOTEVIL-2388587

- https://snyk.io/vuln/SNYK-JS-NOTEVIL-2385946

- https://snyk.io/vuln/SNYK-JS-ARGENCODERSNOTEVIL-2388587

- https://snyk.io/vuln/SNYK-JS-NOTEVIL-2385946

Finding 43 - GHSA-952p-6rrq-rcjv in micromatch:3.1.10

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Medium (5.3)	0.10% / 29.29%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-952p-6rrq-rcjv', 'CVE-2024-4067']	58

Location

Component	Version
micromatch	3.1.10

File Path
/juice-shop/node_modules/micromatch/package.json

CVSS v3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: Regular Expression Denial of Service (ReDoS) in micromatch

Related Vulnerability Description: The NPM package micromatch prior to 4.0.8 is vulnerable to Regular Expression Denial of Service (ReDoS). The vulnerability occurs in micromatch.braces() in index.js because the pattern .* will greedily match anything. By passing a malicious payload, the pattern matching will keep backtracking to the input while it doesn't find the closing bracket. As the input size increases, the consumption time will also increase until it causes the application to hang or slow down. There was a merged fix but further testing shows the issue persists. This issue should be mitigated by using a safe pattern that won't start backtracking the regular expression due to greedy matching. This issue was fixed in version 4.0.8.

Matcher: javascript-matcher

Package URL: pkg:npm/micromatch@3.1.10

Mitigation

Upgrade to version: 4.0.8

References

Vulnerability Datasource: https://github.com/advisories/GHSA-952p-6rrq-rcjv

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2024-4067

Related Vulnerability URLs:

- https://advisory.checkmarx.net/advisory/CVE-2024-4067/

- https://devhub.checkmarx.com/cve-details/CVE-2024-4067/

- https://github.com/micromatch/micromatch/commit/03aa8052171e878897eee5d7bb2ae0ae83ec2ade

- https://github.com/micromatch/micromatch/pull/266

- https://github.com/micromatch/micromatch/releases/tag/4.0.8

- https://devhub.checkmarx.com/cve-details/CVE-2024-4067/

- https://github.com/micromatch/micromatch/blob/2c56a8604b68c1099e7bc0f807ce0865a339747a/index.js#L448

- https://github.com/micromatch/micromatch/issues/243

- https://github.com/micromatch/micromatch/pull/247

Finding 44 - GHSA-cqmj-92xf-r6r9 in socket.io-parser:4.0.5

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Medium (7.3)	0.16% / 37.92%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-cqmj-92xf-r6r9', 'CVE-2023-32695']	53

Location

Component	Version
socket.io-parser	4.0.5

File Path
/juice-shop/node_modules/socket.io-parser/package.json

CVSS v3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: Insufficient validation when decoding a Socket.IO packet

Related Vulnerability Description: socket.io parser is a socket.io encoder and decoder written in JavaScript complying with version 5 of socket.io-protocol. A specially crafted Socket.IO packet can trigger an uncaught exception on the Socket.IO server, thus killing the Node.js process. A patch has been released in version 4.2.3.

Matcher: javascript-matcher

Package URL: pkg:npm/socket.io-parser@4.0.5

Mitigation

Upgrade to version: 4.2.3

References

Vulnerability Datasource: https://github.com/advisories/GHSA-cqmj-92xf-r6r9

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2023-32695

Related Vulnerability URLs:

- https://github.com/socketio/socket.io-parser/commit/2dc3c92622dad113b8676be06f23b1ed46b02ced

- https://github.com/socketio/socket.io-parser/commit/3b78117bf6ba7e99d7a5cfc1ba54d0477554a7f3

- https://github.com/socketio/socket.io-parser/releases/tag/4.2.3

- https://github.com/socketio/socket.io-parser/security/advisories/GHSA-cqmj-92xf-r6r9

- https://github.com/socketio/socket.io-parser/commit/2dc3c92622dad113b8676be06f23b1ed46b02ced

- https://github.com/socketio/socket.io-parser/commit/3b78117bf6ba7e99d7a5cfc1ba54d0477554a7f3

- https://github.com/socketio/socket.io-parser/releases/tag/4.2.3

- https://github.com/socketio/socket.io-parser/security/advisories/GHSA-cqmj-92xf-r6r9

Finding 45 - GHSA-f5x3-32g6-xq36 in tar:4.4.19

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Medium (6.5)	0.20% / 42.24%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-f5x3-32g6-xq36', 'CVE-2024-28863']	52

Location

Component	Version
tar	4.4.19

File Path
/juice-shop/node_modules/node-pre-gyp/node_modules/tar/package.json

CVSS v3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: Denial of service while parsing a tar file due to lack of folders count validation

Related Vulnerability Description: node-tar is a Tar for Node.js. node-tar prior to version 6.2.1 has no limit on the number of sub-folders created in the folder creation process. An attacker who generates a large number of sub-folders can consume memory on the system running node-tar and even crash the Node.js client within few seconds of running it using a path with too many sub-folders inside. Version 6.2.1 fixes this issue by preventing extraction in excessively deep sub-folders.

Matcher: javascript-matcher

Package URL: pkg:npm/tar@4.4.19

Mitigation

Upgrade to version: 6.2.1

References

Vulnerability Datasource: https://github.com/advisories/GHSA-f5x3-32g6-xq36

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2024-28863

Related Vulnerability URLs:

- https://github.com/isaacs/node-tar/commit/fe8cd57da5686f8695415414bda49206a545f7f7

- https://github.com/isaacs/node-tar/security/advisories/GHSA-f5x3-32g6-xq36

- https://security.netapp.com/advisory/ntap-20240524-0005/

- https://github.com/isaacs/node-tar/commit/fe8cd57da5686f8695415414bda49206a545f7f7

- https://github.com/isaacs/node-tar/security/advisories/GHSA-f5x3-32g6-xq36

- https://security.netapp.com/advisory/ntap-20240524-0005/

Finding 46 - GHSA-fvqr-27wr-82fm in lodash:2.4.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Medium (6.5)	0.14% / 34.82%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-fvqr-27wr-82fm', 'CVE-2018-3721']	55

Location

Component	Version
lodash	2.4.2

File Path
/juice-shop/node_modules/sanitize-html/node_modules/lodash/package.json

CVSS v3

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: Prototype Pollution in lodash

Related Vulnerability Description: lodash node module before 4.17.5 suffers from a Modification of Assumed-Immutable Data (MAID) vulnerability via defaultsDeep, merge, and mergeWith functions, which allows a malicious user to modify the prototype of "Object" via **proto**, causing the addition or modification of an existing property that will exist on all objects.

Matcher: javascript-matcher

Package URL: pkg:npm/lodash@2.4.2

Mitigation

Upgrade to version: 4.17.5

References

Vulnerability Datasource: https://github.com/advisories/GHSA-fvqr-27wr-82fm

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2018-3721

Related Vulnerability URLs:

- https://github.com/lodash/lodash/commit/d8e069cc3410082e44eb18fcf8e7f3d08ebe1d4a

- https://hackerone.com/reports/310443

- https://security.netapp.com/advisory/ntap-20190919-0004/

- https://github.com/lodash/lodash/commit/d8e069cc3410082e44eb18fcf8e7f3d08ebe1d4a

- https://hackerone.com/reports/310443

- https://security.netapp.com/advisory/ntap-20190919-0004/

Finding 47 - GHSA-hjrf-2m68-5959 in jsonwebtoken:0.1.0

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Medium (5.0)	0.05% / 14.95%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-hjrf-2m68-5959', 'CVE-2022-23541']	67

Location

Component	Version
jsonwebtoken	0.1.0

File Path
/juice-shop/node_modules/express-jwt/node_modules/jsonwebtoken/package.json

CVSS v3

CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: jsonwebtoken's insecure implementation of key retrieval function could lead to Forgeable Public/Private Tokens from RSA to HMAC

Related Vulnerability Description: jsonwebtoken is an implementation of JSON Web Tokens. Versions <= 8.5.1 of jsonwebtoken library can be misconfigured so that passing a poorly implemented key retrieval function referring to the secretOrPublicKey argument from the readme link will result in incorrect verification of tokens. There is a possibility of using a different algorithm and key combination in verification, other than the one that was used to sign the tokens. Specifically, tokens signed with an asymmetric public key could be verified with a symmetric HS256 algorithm. This can lead to successful validation of forged tokens. If your application is supporting usage of both symmetric key and asymmetric key in jwt.verify() implementation with the same key retrieval function. This issue has been patched, please update to version 9.0.0.

Matcher: javascript-matcher

Package URL: pkg:npm/jsonwebtoken@0.1.0

Mitigation

Upgrade to version: 9.0.0

References

Vulnerability Datasource: https://github.com/advisories/GHSA-hjrf-2m68-5959

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2022-23541

Related Vulnerability URLs:

- https://github.com/auth0/node-jsonwebtoken/commit/e1fa9dcc12054a8681db4e6373da1b30cf7016e3

- https://github.com/auth0/node-jsonwebtoken/releases/tag/v9.0.0

- https://github.com/auth0/node-jsonwebtoken/security/advisories/GHSA-hjrf-2m68-5959

- https://security.netapp.com/advisory/ntap-20240621-0007/

- https://github.com/auth0/node-jsonwebtoken/commit/e1fa9dcc12054a8681db4e6373da1b30cf7016e3

- https://github.com/auth0/node-jsonwebtoken/releases/tag/v9.0.0

- https://github.com/auth0/node-jsonwebtoken/security/advisories/GHSA-hjrf-2m68-5959

- https://security.netapp.com/advisory/ntap-20240621-0007/

Finding 48 - GHSA-hjrf-2m68-5959 in jsonwebtoken:0.4.0

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Medium (5.0)	0.05% / 14.95%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-hjrf-2m68-5959', 'CVE-2022-23541']	68

Location

Component	Version
jsonwebtoken	0.4.0

File Path
/juice-shop/node_modules/jsonwebtoken/package.json

CVSS v3

CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: jsonwebtoken's insecure implementation of key retrieval function could lead to Forgeable Public/Private Tokens from RSA to HMAC

Related Vulnerability Description: jsonwebtoken is an implementation of JSON Web Tokens. Versions <= 8.5.1 of jsonwebtoken library can be misconfigured so that passing a poorly implemented key retrieval function referring to the secretOrPublicKey argument from the readme link will result in incorrect verification of tokens. There is a possibility of using a different algorithm and key combination in verification, other than the one that was used to sign the tokens. Specifically, tokens signed with an asymmetric public key could be verified with a symmetric HS256 algorithm. This can lead to successful validation of forged tokens. If your application is supporting usage of both symmetric key and asymmetric key in jwt.verify() implementation with the same key retrieval function. This issue has been patched, please update to version 9.0.0.

Matcher: javascript-matcher

Package URL: pkg:npm/jsonwebtoken@0.4.0

Mitigation

Upgrade to version: 9.0.0

References

Vulnerability Datasource: https://github.com/advisories/GHSA-hjrf-2m68-5959

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2022-23541

Related Vulnerability URLs:

- https://github.com/auth0/node-jsonwebtoken/commit/e1fa9dcc12054a8681db4e6373da1b30cf7016e3

- https://github.com/auth0/node-jsonwebtoken/releases/tag/v9.0.0

- https://github.com/auth0/node-jsonwebtoken/security/advisories/GHSA-hjrf-2m68-5959

- https://security.netapp.com/advisory/ntap-20240621-0007/

- https://github.com/auth0/node-jsonwebtoken/commit/e1fa9dcc12054a8681db4e6373da1b30cf7016e3

- https://github.com/auth0/node-jsonwebtoken/releases/tag/v9.0.0

- https://github.com/auth0/node-jsonwebtoken/security/advisories/GHSA-hjrf-2m68-5959

- https://security.netapp.com/advisory/ntap-20240621-0007/

Finding 49 - GHSA-mjxr-4v3x-q3m4 in sanitize-html:1.4.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Medium (5.3)	0.29% / 52.12%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-mjxr-4v3x-q3m4', 'CVE-2021-26540']	47

Location

Component	Version
sanitize-html	1.4.2

File Path
/juice-shop/node_modules/sanitize-html/package.json

CVSS v3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: Improper Input Validation in sanitize-html

Related Vulnerability Description: Apostrophe Technologies sanitize-html before 2.3.2 does not properly validate the hostnames set by the "allowedIframeHostnames" option when the "allowIframeRelativeUrls" is set to true, which allows attackers to bypass hostname whitelist for iframe element, related using an src value that starts with "/\example.com".

Matcher: javascript-matcher

Package URL: pkg:npm/sanitize-html@1.4.2

Mitigation

Upgrade to version: 2.3.2

References

Vulnerability Datasource: https://github.com/advisories/GHSA-mjxr-4v3x-q3m4

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2021-26540

Related Vulnerability URLs:

- https://advisory.checkmarx.net/advisory/CX-2021-4309

- https://github.com/apostrophecms/sanitize-html/blob/main/CHANGELOG.md#232-2021-01-26

- https://github.com/apostrophecms/sanitize-html/pull/460

- https://advisory.checkmarx.net/advisory/CX-2021-4309

- https://github.com/apostrophecms/sanitize-html/blob/main/CHANGELOG.md#232-2021-01-26

- https://github.com/apostrophecms/sanitize-html/pull/460

Finding 50 - GHSA-p5gc-c584-jj6v in vm2:3.9.17

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Medium (5.3)	0.65% / 70.15%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-p5gc-c584-jj6v', 'CVE-2023-32313']	41

Location

Component	Version
vm2	3.9.17

File Path
/juice-shop/node_modules/vm2/package.json

CVSS v3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: vm2 vulnerable to Inspect Manipulation

Related Vulnerability Description: vm2 is a sandbox that can run untrusted code with Node's built-in modules. In versions 3.9.17 and lower of vm2 it was possible to get a read-write reference to the node inspect method and edit options for console.log. As a result a threat actor can edit options for the console.log command. This vulnerability was patched in the release of version 3.9.18 of vm2. Users are advised to upgrade. Users unable to upgrade may make the inspect method readonly with vm.readonly(inspect) after creating a vm.

Matcher: javascript-matcher

Package URL: pkg:npm/vm2@3.9.17

Mitigation

Upgrade to version: 3.9.18

References

Vulnerability Datasource: https://github.com/advisories/GHSA-p5gc-c584-jj6v

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2023-32313

Related Vulnerability URLs:

- https://gist.github.com/arkark/c1c57eaf3e0a649af1a70c2b93b17550

- https://github.com/patriksimek/vm2/commit/5206ba25afd86ef547a2c9d48d46ca7a9e6ec238

- https://github.com/patriksimek/vm2/releases/tag/3.9.18

- https://github.com/patriksimek/vm2/security/advisories/GHSA-p5gc-c584-jj6v

- https://gist.github.com/arkark/c1c57eaf3e0a649af1a70c2b93b17550

- https://github.com/patriksimek/vm2/commit/5206ba25afd86ef547a2c9d48d46ca7a9e6ec238

- https://github.com/patriksimek/vm2/releases/tag/3.9.18

- https://github.com/patriksimek/vm2/security/advisories/GHSA-p5gc-c584-jj6v

Finding 51 - GHSA-pfrx-2q88-qq97 in got:8.3.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Medium (5.3)	0.79% / 73.15%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-pfrx-2q88-qq97', 'CVE-2022-33987']	39

Location

Component	Version
got	8.3.2

File Path
/juice-shop/node_modules/got/package.json

CVSS v3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: Got allows a redirect to a UNIX socket

Related Vulnerability Description: The got package before 12.1.0 (also fixed in 11.8.5) for Node.js allows a redirect to a UNIX socket.

Matcher: javascript-matcher

Package URL: pkg:npm/got@8.3.2

Mitigation

Upgrade to version: 11.8.5

References

Vulnerability Datasource: https://github.com/advisories/GHSA-pfrx-2q88-qq97

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2022-33987

Related Vulnerability URLs:

- https://github.com/sindresorhus/got/compare/v12.0.3...v12.1.0

- https://github.com/sindresorhus/got/pull/2047

- https://github.com/sindresorhus/got/releases/tag/v11.8.5

- https://github.com/sindresorhus/got/compare/v12.0.3...v12.1.0

- https://github.com/sindresorhus/got/pull/2047

- https://github.com/sindresorhus/got/releases/tag/v11.8.5

Finding 52 - GHSA-qhxp-v273-g94h in sanitize-html:1.4.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Medium (6.1)	0.03% / 7.49%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-qhxp-v273-g94h', 'CVE-2019-25225']	73

Location

Component	Version
sanitize-html	1.4.2

File Path
/juice-shop/node_modules/sanitize-html/package.json

CVSS v3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: sanitize-html is vulnerable to XSS through incomprehensive sanitization

Related Vulnerability Description: sanitize-html prior to version 2.0.0-beta is vulnerable to Cross-site Scripting (XSS). The sanitizeHtml() function in index.js does not sanitize content when using the custom transformTags option, which is intended to convert attribute values into text. As a result, malicious input can be transformed into executable code.

Matcher: javascript-matcher

Package URL: pkg:npm/sanitize-html@1.4.2

Mitigation

Upgrade to version: 2.0.0-beta

References

Vulnerability Datasource: https://github.com/advisories/GHSA-qhxp-v273-g94h

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2019-25225

Related Vulnerability URLs:

- https://github.com/Checkmarx/Vulnerabilities-Proofs-of-Concept/tree/main/2019/CVE-2019-25225

- https://github.com/apostrophecms/sanitize-html/commit/712cb6895825c8bb6ede71a16b42bade42abcaf3

- https://github.com/apostrophecms/sanitize-html/issues/293

- https://github.com/apostrophecms/sanitize-html/pull/156

Finding 53 - GHSA-qwph-4952-7xr6 in jsonwebtoken:0.1.0

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Medium (6.4)	0.02% / 2.68%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-qwph-4952-7xr6', 'CVE-2022-23540']	78

Location

Component	Version
jsonwebtoken	0.1.0

File Path
/juice-shop/node_modules/express-jwt/node_modules/jsonwebtoken/package.json

CVSS v3

CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:H/A:L

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: jsonwebtoken vulnerable to signature validation bypass due to insecure default algorithm in jwt.verify()

Related Vulnerability Description: In versions <=8.5.1 of jsonwebtoken library, lack of algorithm definition in the jwt.verify() function can lead to signature validation bypass due to defaulting to the none algorithm for signature verification. Users are affected if you do not specify algorithms in the jwt.verify() function. This issue has been fixed, please update to version 9.0.0 which removes the default support for the none algorithm in the jwt.verify() method. There will be no impact, if you update to version 9.0.0 and you don't need to allow for the none algorithm. If you need 'none' algorithm, you have to explicitly specify that in jwt.verify() options.

Matcher: javascript-matcher

Package URL: pkg:npm/jsonwebtoken@0.1.0

Mitigation

Upgrade to version: 9.0.0

References

Vulnerability Datasource: https://github.com/advisories/GHSA-qwph-4952-7xr6

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2022-23540

Related Vulnerability URLs:

- https://github.com/auth0/node-jsonwebtoken/commit/e1fa9dcc12054a8681db4e6373da1b30cf7016e3

- https://github.com/auth0/node-jsonwebtoken/security/advisories/GHSA-qwph-4952-7xr6

- https://security.netapp.com/advisory/ntap-20240621-0007/

- https://github.com/auth0/node-jsonwebtoken/commit/e1fa9dcc12054a8681db4e6373da1b30cf7016e3

- https://github.com/auth0/node-jsonwebtoken/security/advisories/GHSA-qwph-4952-7xr6

- https://security.netapp.com/advisory/ntap-20240621-0007/

Finding 54 - GHSA-qwph-4952-7xr6 in jsonwebtoken:0.4.0

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Medium (6.4)	0.02% / 2.68%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-qwph-4952-7xr6', 'CVE-2022-23540']	79

Location

Component	Version
jsonwebtoken	0.4.0

File Path
/juice-shop/node_modules/jsonwebtoken/package.json

CVSS v3

CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:H/A:L

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: jsonwebtoken vulnerable to signature validation bypass due to insecure default algorithm in jwt.verify()

Related Vulnerability Description: In versions <=8.5.1 of jsonwebtoken library, lack of algorithm definition in the jwt.verify() function can lead to signature validation bypass due to defaulting to the none algorithm for signature verification. Users are affected if you do not specify algorithms in the jwt.verify() function. This issue has been fixed, please update to version 9.0.0 which removes the default support for the none algorithm in the jwt.verify() method. There will be no impact, if you update to version 9.0.0 and you don’t need to allow for the none algorithm. If you need 'none' algorithm, you have to explicitly specify that in jwt.verify() options.

Matcher: javascript-matcher

Package URL: pkg:npm/jsonwebtoken@0.4.0

Mitigation

Upgrade to version: 9.0.0

References

Vulnerability Datasource: https://github.com/advisories/GHSA-qwph-4952-7xr6

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2022-23540

Related Vulnerability URLs:

- https://github.com/auth0/node-jsonwebtoken/commit/e1fa9dcc12054a8681db4e6373da1b30cf7016e3

- https://github.com/auth0/node-jsonwebtoken/security/advisories/GHSA-qwph-4952-7xr6

- https://security.netapp.com/advisory/ntap-20240621-0007/

- https://github.com/auth0/node-jsonwebtoken/commit/e1fa9dcc12054a8681db4e6373da1b30cf7016e3

- https://github.com/auth0/node-jsonwebtoken/security/advisories/GHSA-qwph-4952-7xr6

- https://security.netapp.com/advisory/ntap-20240621-0007/

Finding 55 - GHSA-r7qp-cfhv-p84w in engine.io:4.1.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Medium (6.5)	2.78% / 85.57%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-r7qp-cfhv-p84w', 'CVE-2022-41940']	32

Location

Component	Version
engine.io	4.1.2

File Path
/juice-shop/node_modules/engine.io/package.json

CVSS v3

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: Uncaught exception in engine.io

Related Vulnerability Description: Engine.IO is the implementation of transport-based cross-browser/cross-device bi-directional communication layer for Socket.IO. A specially crafted HTTP request can trigger an uncaught exception on the Engine.IO server, thus killing the Node.js process. This impacts all the users of the engine.io package, including those who uses depending packages like socket.io. There is no known workaround except upgrading to a safe version. There are patches for this issue released in versions 3.6.1 and 6.2.1.

Matcher: javascript-matcher

Package URL: pkg:npm/engine.io@4.1.2

Mitigation

Upgrade to version: 6.2.1

References

Vulnerability Datasource: https://github.com/advisories/GHSA-r7qp-cfhv-p84w

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2022-41940

Related Vulnerability URLs:

- https://github.com/socketio/engine.io/commit/425e833ab13373edf1dd5a0706f07100db14e3c6

- https://github.com/socketio/engine.io/commit/83c4071af871fc188298d7d591e95670bf9f9085

- https://github.com/socketio/engine.io/security/advisories/GHSA-r7qp-cfhv-p84w

- https://github.com/socketio/engine.io/commit/425e833ab13373edf1dd5a0706f07100db14e3c6

- https://github.com/socketio/engine.io/commit/83c4071af871fc188298d7d591e95670bf9f9085

- https://github.com/socketio/engine.io/security/advisories/GHSA-r7qp-cfhv-p84w

Finding 56 - GHSA-rjqq-98f6-6j3r in sanitize-html:1.4.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Medium (5.3)	0.29% / 52.12%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-rjqq-98f6-6j3r', 'CVE-2021-26539']	48

Location

Component	Version
sanitize-html	1.4.2

File Path
/juice-shop/node_modules/sanitize-html/package.json

CVSS v3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: Improper Input Validation in sanitize-html

Related Vulnerability Description: 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.

Matcher: javascript-matcher

Package URL: pkg:npm/sanitize-html@1.4.2

Mitigation

Upgrade to version: 2.3.1

References

Vulnerability Datasource: https://github.com/advisories/GHSA-rjqq-98f6-6j3r

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2021-26539

Related Vulnerability URLs:

- https://advisory.checkmarx.net/advisory/CX-2021-4308

- https://github.com/apostrophecms/sanitize-html/blob/main/CHANGELOG.md#231-2021-01-22

- https://github.com/apostrophecms/sanitize-html/pull/458

- https://advisory.checkmarx.net/advisory/CX-2021-4308

- https://github.com/apostrophecms/sanitize-html/blob/main/CHANGELOG.md#231-2021-01-22

- https://github.com/apostrophecms/sanitize-html/pull/458

Finding 57 - GHSA-rm97-x556-q36h in sanitize-html:1.4.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Medium (5.3)	1.34% / 79.41%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-rm97-x556-q36h', 'CVE-2024-21501']	37

Location

Component	Version
sanitize-html	1.4.2

File Path
/juice-shop/node_modules/sanitize-html/package.json

CVSS v3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: sanitize-html Information Exposure vulnerability

Related Vulnerability Description: Versions of the package sanitize-html before 2.12.1 are vulnerable to Information Exposure when used on the backend and with the style attribute allowed, allowing enumeration of files in the system (including project dependencies). An attacker could exploit this vulnerability to gather details about the file system structure and dependencies of the targeted server.

Matcher: javascript-matcher

Package URL: pkg:npm/sanitize-html@1.4.2

Mitigation

Upgrade to version: 2.12.1

References

Vulnerability Datasource: https://github.com/advisories/GHSA-rm97-x556-q36h

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2024-21501

Related Vulnerability URLs:

- https://gist.github.com/Slonser/8b4d061abe6ee1b2e10c7242987674cf

- https://github.com/apostrophecms/apostrophe/discussions/4436

- https://github.com/apostrophecms/sanitize-html/commit/c5dbdf77fe8b836d3bf4554ea39edb45281ec0b4

- https://github.com/apostrophecms/sanitize-html/pull/650

- https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/4EB5JPYRCTS64EA5AMV3INHDPI6I4AW7/

- https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/P4I5X6V3LYUNBMZ5YOW4BV427TH3IK4S/

- https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-6276557

- https://security.snyk.io/vuln/SNYK-JS-SANITIZEHTML-6256334

- https://gist.github.com/Slonser/8b4d061abe6ee1b2e10c7242987674cf

- https://github.com/apostrophecms/apostrophe/discussions/4436

- https://github.com/apostrophecms/sanitize-html/commit/c5dbdf77fe8b836d3bf4554ea39edb45281ec0b4

- https://github.com/apostrophecms/sanitize-html/pull/650

- https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/4EB5JPYRCTS64EA5AMV3INHDPI6I4AW7/

- https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/P4I5X6V3LYUNBMZ5YOW4BV427TH3IK4S/

- https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-6276557

- https://security.snyk.io/vuln/SNYK-JS-SANITIZEHTML-6256334

Finding 58 - GHSA-rvg8-pwq2-xj7q in base64url:0.0.6

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Medium	N.A. / N.A.	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-rvg8-pwq2-xj7q']	90

Location

Component	Version
base64url	0.0.6

File Path
/juice-shop/node_modules/base64url/package.json

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: Out-of-bounds Read in base64url

Matcher: javascript-matcher

Package URL: pkg:npm/base64url@0.0.6

Mitigation

Upgrade to version: 3.0.0

References

Vulnerability Datasource: https://github.com/advisories/GHSA-rvg8-pwq2-xj7q

Finding 59 - GHSA-xc6g-ggrc-qq4r in sanitize-html:1.4.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Medium (6.1)	0.29% / 51.89%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-xc6g-ggrc-qq4r', 'CVE-2017-16016']	49

Location

Component	Version
sanitize-html	1.4.2

File Path
/juice-shop/node_modules/sanitize-html/package.json

CVSS v3

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: Cross-Site Scripting in sanitize-html

Related Vulnerability Description: Sanitize-html is a library for scrubbing html input of malicious values. Versions 1.11.1 and below are vulnerable to cross site scripting (XSS) in certain scenarios: If allowed at least one nonTextTags, the result is a potential XSS vulnerability.

Matcher: javascript-matcher

Package URL: pkg:npm/sanitize-html@1.4.2

Mitigation

Upgrade to version: 1.11.4

References

Vulnerability Datasource: https://github.com/advisories/GHSA-xc6g-ggrc-qq4r

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2017-16016

Related Vulnerability URLs:

- https://github.com/punkave/sanitize-html/commit/5d205a1005ba0df80e21d8c64a15bb3accdb2403

- https://github.com/punkave/sanitize-html/issues/100

- https://nodesecurity.io/advisories/154

- https://github.com/punkave/sanitize-html/commit/5d205a1005ba0df80e21d8c64a15bb3accdb2403

- https://github.com/punkave/sanitize-html/issues/100

- https://nodesecurity.io/advisories/154

Finding 60 - generic.html-templates.security.unquoted-attribute-var.unquoted-attribute-var

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active	Nov. 12, 2025	0 days	Admin User (admin)	79	7

Location

Line Number
40

File Path
/src/frontend/src/app/search-result/search-result.component.html

Description

Result message: Detected a unquoted template variable as an attribute. If unquoted, a malicious actor could inject custom JavaScript handlers. To fix this, add quotes around the template expression, like this: "{{ expr }}".

References

https://flask.palletsprojects.com/en/1.1.x/security/#cross-site-scripting-xss

Finding 61 - generic.html-templates.security.unquoted-attribute-var.unquoted-attribute-var

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active	Nov. 12, 2025	0 days	Admin User (admin)	79	25

Location

Line Number
21

File Path
/src/views/dataErasureForm.hbs

Description

Result message: Detected a unquoted template variable as an attribute. If unquoted, a malicious actor could inject custom JavaScript handlers. To fix this, add quotes around the template expression, like this: "{{ expr }}".

References

https://flask.palletsprojects.com/en/1.1.x/security/#cross-site-scripting-xss

Finding 62 - generic.html-templates.security.unquoted-attribute-var.unquoted-attribute-var

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active	Nov. 12, 2025	0 days	Admin User (admin)	79	6

Location

Line Number
15

File Path
/src/frontend/src/app/purchase-basket/purchase-basket.component.html

Description

Result message: Detected a unquoted template variable as an attribute. If unquoted, a malicious actor could inject custom JavaScript handlers. To fix this, add quotes around the template expression, like this: "{{ expr }}".

References

https://flask.palletsprojects.com/en/1.1.x/security/#cross-site-scripting-xss

Finding 63 - generic.html-templates.security.unquoted-attribute-var.unquoted-attribute-var

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active	Nov. 12, 2025	0 days	Admin User (admin)	79	5

Location

Line Number
17

File Path
/src/frontend/src/app/navbar/navbar.component.html

Description

Result message: Detected a unquoted template variable as an attribute. If unquoted, a malicious actor could inject custom JavaScript handlers. To fix this, add quotes around the template expression, like this: "{{ expr }}".

References

https://flask.palletsprojects.com/en/1.1.x/security/#cross-site-scripting-xss

Finding 64 - javascript.express.security.audit.express-check-directory-listing.express-check-directory-listing

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active	Nov. 12, 2025	0 days	Admin User (admin)	548	23

Location

Line Number
277

File Path
/src/server.ts

Description

Result message: Directory listing/indexing is enabled, which may lead to disclosure of sensitive directories and files. It is recommended to disable directory listing unless it is a public resource. If you need directory listing, ensure that sensitive files are inaccessible when querying the resource.

References

https://www.npmjs.com/package/serve-index

https://www.acunetix.com/blog/articles/directory-listing-information-disclosure/

Finding 65 - javascript.express.security.audit.express-check-directory-listing.express-check-directory-listing

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active	Nov. 12, 2025	0 days	Admin User (admin)	548	24

Location

Line Number
281

File Path
/src/server.ts

Description

Result message: Directory listing/indexing is enabled, which may lead to disclosure of sensitive directories and files. It is recommended to disable directory listing unless it is a public resource. If you need directory listing, ensure that sensitive files are inaccessible when querying the resource.

References

https://www.npmjs.com/package/serve-index

https://www.acunetix.com/blog/articles/directory-listing-information-disclosure/

Finding 66 - javascript.express.security.audit.express-check-directory-listing.express-check-directory-listing

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active	Nov. 12, 2025	0 days	Admin User (admin)	548	22

Location

Line Number
273

File Path
/src/server.ts

Description

Result message: Directory listing/indexing is enabled, which may lead to disclosure of sensitive directories and files. It is recommended to disable directory listing unless it is a public resource. If you need directory listing, ensure that sensitive files are inaccessible when querying the resource.

References

https://www.npmjs.com/package/serve-index

https://www.acunetix.com/blog/articles/directory-listing-information-disclosure/

Finding 67 - javascript.express.security.audit.express-check-directory-listing.express-check-directory-listing

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active	Nov. 12, 2025	0 days	Admin User (admin)	548	21

Location

Line Number
269

File Path
/src/server.ts

Description

Result message: Directory listing/indexing is enabled, which may lead to disclosure of sensitive directories and files. It is recommended to disable directory listing unless it is a public resource. If you need directory listing, ensure that sensitive files are inaccessible when querying the resource.

References

https://www.npmjs.com/package/serve-index

https://www.acunetix.com/blog/articles/directory-listing-information-disclosure/

Finding 68 - javascript.express.security.audit.express-open-redirect.express-open-redirect

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active	Nov. 12, 2025	0 days	Admin User (admin)	601	16

Location

Line Number
19

File Path
/src/routes/redirect.ts

Description

Result message: The application redirects to a URL specified by user-supplied input query that is not validated. This could redirect users to malicious locations. Consider using an allow-list approach to validate URLs, or warn users they are being redirected to a third-party website.

References

https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html

Finding 69 - javascript.express.security.audit.express-res-sendfile.express-res-sendfile

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active	Nov. 12, 2025	0 days	Admin User (admin)	73	12

Location

Line Number
14

File Path
/src/routes/logfileServer.ts

Description

Result message: The application processes user-input, this is passed to res.sendFile which can allow an attacker to arbitrarily read files on the system through path traversal. It is recommended to perform input validation in addition to canonicalizing the path. This allows you to validate the path against the intended directory it should be accessing.

References

https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html

Finding 70 - javascript.express.security.audit.express-res-sendfile.express-res-sendfile

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active	Nov. 12, 2025	0 days	Admin User (admin)	73	10

Location

Line Number
33

File Path
/src/routes/fileServer.ts

Description

Result message: The application processes user-input, this is passed to res.sendFile which can allow an attacker to arbitrarily read files on the system through path traversal. It is recommended to perform input validation in addition to canonicalizing the path. This allows you to validate the path against the intended directory it should be accessing.

References

https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html

Finding 71 - javascript.express.security.audit.express-res-sendfile.express-res-sendfile

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active	Nov. 12, 2025	0 days	Admin User (admin)	73	11

Location

Line Number
14

File Path
/src/routes/keyServer.ts

Description

Result message: The application processes user-input, this is passed to res.sendFile which can allow an attacker to arbitrarily read files on the system through path traversal. It is recommended to perform input validation in addition to canonicalizing the path. This allows you to validate the path against the intended directory it should be accessing.

References

https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html

Finding 72 - javascript.express.security.audit.express-res-sendfile.express-res-sendfile

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active	Nov. 12, 2025	0 days	Admin User (admin)	73	14

Location

Line Number
14

File Path
/src/routes/quarantineServer.ts

Description

Result message: The application processes user-input, this is passed to res.sendFile which can allow an attacker to arbitrarily read files on the system through path traversal. It is recommended to perform input validation in addition to canonicalizing the path. This allows you to validate the path against the intended directory it should be accessing.

References

https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html

Finding 73 - javascript.express.security.audit.possible-user-input-redirect.unknown-value-in-redirect

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active	Nov. 12, 2025	0 days	Admin User (admin)	601	15

Location

Line Number
19

File Path
/src/routes/redirect.ts

Description

Result message: It looks like 'toUrl' is read from user input and it is used to as a redirect. Ensure 'toUrl' is not externally controlled, otherwise this is an open redirect.

References

https://owasp.org/Top10/A01_2021-Broken_Access_Control

Finding 74 - javascript.express.security.injection.raw-html-format.raw-html-format

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active	Nov. 12, 2025	0 days	Admin User (admin)	79	9

Location

Line Number
197

File Path
/src/routes/chatbot.ts

Description

Result message: User data flows into the host portion of this manually-constructed HTML. This can introduce a Cross-Site-Scripting (XSS) vulnerability if this comes from user-provided input. Consider using a sanitization library such as DOMPurify to sanitize the HTML within.

References

https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html

Finding 75 - javascript.jsonwebtoken.security.jwt-hardcode.hardcoded-jwt-secret

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active	Nov. 12, 2025	0 days	Admin User (admin)	798	8

Location

Line Number
56

File Path
/src/lib/insecurity.ts

Description

Result message: A hard-coded credential was detected. It is not recommended to store credentials in source-code, as this risks secrets being leaked and used by either an internal or external malicious adversary. It is recommended to use environment variables to securely provide credentials or retrieve credentials from a secure vault or HSM (Hardware Security Module).

References

https://cheatsheetseries.owasp.org/cheatsheets/Secrets_Management_Cheat_Sheet.html

Finding 76 - javascript.lang.security.audit.unknown-value-with-script-tag.unknown-value-with-script-tag

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active	Nov. 12, 2025	0 days	Admin User (admin)	79	20

Location

Line Number
71

File Path
/src/routes/videoHandler.ts

Description

Result message: Cannot determine what 'subs' is and it is used with a '<script>' tag. This could be susceptible to cross-site scripting (XSS). Ensure 'subs' is not externally controlled, or sanitize this data.

References

https://www.developsec.com/2017/11/09/xss-in-a-script-tag/

https://github.com/juice-shop/juice-shop/blob/1ceb8751e986dacd3214a618c37e7411be6bc11a/routes/videoHandler.ts#L68

Finding 77 - javascript.lang.security.audit.unknown-value-with-script-tag.unknown-value-with-script-tag

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active	Nov. 12, 2025	0 days	Admin User (admin)	79	19

Location

Line Number
58

File Path
/src/routes/videoHandler.ts

Description

Result message: Cannot determine what 'subs' is and it is used with a '<script>' tag. This could be susceptible to cross-site scripting (XSS). Ensure 'subs' is not externally controlled, or sanitize this data.

References

https://www.developsec.com/2017/11/09/xss-in-a-script-tag/

https://github.com/juice-shop/juice-shop/blob/1ceb8751e986dacd3214a618c37e7411be6bc11a/routes/videoHandler.ts#L68

Low

Finding 78 - GHSA-pxg6-pf52-xh8x in cookie:0.4.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Low	0.07% / 21.76%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['GHSA-pxg6-pf52-xh8x', 'CVE-2024-47764']	69

Location

Component	Version
cookie	0.4.2

File Path
/juice-shop/node_modules/engine.io/node_modules/cookie/package.json

Description

Vulnerability Namespace: github:language:javascript

Vulnerability Description: cookie accepts cookie name, path, and domain with out of bounds characters

Related Vulnerability Description: cookie is a basic HTTP cookie parser and serializer for HTTP servers. The cookie name could be used to set other fields of the cookie, resulting in an unexpected cookie value. A similar escape can be used for path and domain, which could be abused to alter other fields of the cookie. Upgrade to 0.7.0, which updates the validation for name, path, and domain.

Matcher: javascript-matcher

Package URL: pkg:npm/cookie@0.4.2

Mitigation

Upgrade to version: 0.7.0

References

Vulnerability Datasource: https://github.com/advisories/GHSA-pxg6-pf52-xh8x

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2024-47764

Related Vulnerability URLs:

- https://github.com/jshttp/cookie/commit/e10042845354fea83bd8f34af72475eed1dadf5c

- https://github.com/jshttp/cookie/pull/167

- https://github.com/jshttp/cookie/security/advisories/GHSA-pxg6-pf52-xh8x

Info

Finding 79 - CVE-2010-4756 in libc6:2.36-9+deb12u10

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Info	0.37% / 58.43%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['CVE-2010-4756']	71

Location

Component	Version
libc6	2.36-9+deb12u10

File Path
/var/lib/dpkg/status.d/libc6

Description

Vulnerability Namespace: debian:distro:debian:12

Vulnerability Description: The glob implementation in the GNU C Library (aka glibc or libc6) allows remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in STAT commands to an FTP daemon, a different vulnerability than CVE-2010-2632.

Matcher: dpkg-matcher

Package URL: pkg:deb/debian/libc6@2.36-9%2Bdeb12u10?arch=arm64&distro=debian-12&upstream=glibc

References

Vulnerability Datasource: https://security-tracker.debian.org/tracker/CVE-2010-4756

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2010-4756

Related Vulnerability URLs:

- http://cxib.net/stuff/glob-0day.c

- http://securityreason.com/achievement_securityalert/89

- http://securityreason.com/exploitalert/9223

- https://bugzilla.redhat.com/show_bug.cgi?id=681681

- https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2010-4756

- http://cxib.net/stuff/glob-0day.c

- http://securityreason.com/achievement_securityalert/89

- http://securityreason.com/exploitalert/9223

- https://bugzilla.redhat.com/show_bug.cgi?id=681681

- https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2010-4756

Finding 80 - CVE-2018-20796 in libc6:2.36-9+deb12u10

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Info (7.5)	1.84% / 82.34%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['CVE-2018-20796']	54

Location

Component	Version
libc6	2.36-9+deb12u10

File Path
/var/lib/dpkg/status.d/libc6

CVSS v3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description

Vulnerability Namespace: debian:distro:debian:12

Vulnerability Description: In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/regexec.c has Uncontrolled Recursion, as demonstrated by '(\227|)(\1\1|t1|\\2537)+' in grep.

Matcher: dpkg-matcher

Package URL: pkg:deb/debian/libc6@2.36-9%2Bdeb12u10?arch=arm64&distro=debian-12&upstream=glibc

References

Vulnerability Datasource: https://security-tracker.debian.org/tracker/CVE-2018-20796

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2018-20796

Related Vulnerability URLs:

- http://www.securityfocus.com/bid/107160

- https://debbugs.gnu.org/cgi/bugreport.cgi?bug=34141

- https://lists.gnu.org/archive/html/bug-gnulib/2019-01/msg00108.html

- https://security.netapp.com/advisory/ntap-20190315-0002/

- https://support.f5.com/csp/article/K26346590?utm_source=f5support&amp%3Butm_medium=RSS

- http://www.securityfocus.com/bid/107160

- https://debbugs.gnu.org/cgi/bugreport.cgi?bug=34141

- https://lists.gnu.org/archive/html/bug-gnulib/2019-01/msg00108.html

- https://security.netapp.com/advisory/ntap-20190315-0002/

- https://support.f5.com/csp/article/K26346590?utm_source=f5support&amp%3Butm_medium=RSS

Finding 81 - CVE-2019-1010022 in libc6:2.36-9+deb12u10

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Info (9.8)	0.14% / 35.66%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['CVE-2019-1010022']	81

Location

Component	Version
libc6	2.36-9+deb12u10

File Path
/var/lib/dpkg/status.d/libc6

CVSS v3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description

Vulnerability Namespace: debian:distro:debian:12

Vulnerability Description: GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass stack guard protection. The component is: nptl. The attack vector is: Exploit stack buffer overflow vulnerability and use this bypass vulnerability to bypass stack guard. NOTE: Upstream comments indicate "this is being treated as a non-security bug and no real threat.

Matcher: dpkg-matcher

Package URL: pkg:deb/debian/libc6@2.36-9%2Bdeb12u10?arch=arm64&distro=debian-12&upstream=glibc

References

Vulnerability Datasource: https://security-tracker.debian.org/tracker/CVE-2019-1010022

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2019-1010022

Related Vulnerability URLs:

- https://sourceware.org/bugzilla/show_bug.cgi?id=22850

- https://sourceware.org/bugzilla/show_bug.cgi?id=22850#c3

- https://ubuntu.com/security/CVE-2019-1010022

- https://sourceware.org/bugzilla/show_bug.cgi?id=22850

- https://sourceware.org/bugzilla/show_bug.cgi?id=22850#c3

- https://ubuntu.com/security/CVE-2019-1010022

Finding 82 - CVE-2019-1010023 in libc6:2.36-9+deb12u10

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Info (8.8)	0.72% / 71.81%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['CVE-2019-1010023']	64

Location

Component	Version
libc6	2.36-9+deb12u10

File Path
/var/lib/dpkg/status.d/libc6

CVSS v3

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Description

Vulnerability Namespace: debian:distro:debian:12

Vulnerability Description: GNU Libc current is affected by: Re-mapping current loaded library with malicious ELF file. The impact is: In worst case attacker may evaluate privileges. The component is: libld. The attack vector is: Attacker sends 2 ELF files to victim and asks to run ldd on it. ldd execute code. NOTE: Upstream comments indicate "this is being treated as a non-security bug and no

real threat.

Matcher: dpkg-matcher

Package URL: pkg:deb/debian/libc6@2.36-9%2Bdeb12u10?arch=arm64&distro=debian-12&upstream=glibc

References

Vulnerability Datasource: https://security-tracker.debian.org/tracker/CVE-2019-1010023

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2019-1010023

Related Vulnerability URLs:

- http://www.securityfocus.com/bid/109167

- https://sourceware.org/bugzilla/show_bug.cgi?id=22851

- https://support.f5.com/csp/article/K11932200?utm_source=f5support&amp%3Butm_medium=RSS

- https://ubuntu.com/security/CVE-2019-1010023

- http://www.securityfocus.com/bid/109167

- https://sourceware.org/bugzilla/show_bug.cgi?id=22851

- https://support.f5.com/csp/article/K11932200?utm_source=f5support&amp%3Butm_medium=RSS

- https://ubuntu.com/security/CVE-2019-1010023

Finding 83 - CVE-2019-1010024 in libc6:2.36-9+deb12u10

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Info (5.3)	0.38% / 58.54%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['CVE-2019-1010024']	70

Location

Component	Version
libc6	2.36-9+deb12u10

File Path
/var/lib/dpkg/status.d/libc6

CVSS v3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Description

Vulnerability Namespace: debian:distro:debian:12

Vulnerability Description: GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass ASLR using cache of thread stack and heap. The component is: glibc. NOTE: Upstream comments indicate "this is being treated as a non-security bug and no real threat.

Matcher: dpkg-matcher

Package URL: pkg:deb/debian/libc6@2.36-9%2Bdeb12u10?arch=arm64&distro=debian-12&upstream=glibc

References

Vulnerability Datasource: https://security-tracker.debian.org/tracker/CVE-2019-1010024

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2019-1010024

Related Vulnerability URLs:

- http://www.securityfocus.com/bid/109162

- https://sourceware.org/bugzilla/show_bug.cgi?id=22852

- https://support.f5.com/csp/article/K06046097

- https://support.f5.com/csp/article/K06046097?utm_source=f5support&amp%3Butm_medium=RSS

- https://ubuntu.com/security/CVE-2019-1010024

- http://www.securityfocus.com/bid/109162

- https://sourceware.org/bugzilla/show_bug.cgi?id=22852

- https://support.f5.com/csp/article/K06046097

- https://support.f5.com/csp/article/K06046097?utm_source=f5support&amp%3Butm_medium=RSS

- https://ubuntu.com/security/CVE-2019-1010024

Finding 84 - CVE-2019-1010025 in libc6:2.36-9+deb12u10

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Info (5.3)	0.23% / 45.78%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['CVE-2019-1010025']	77

Location

Component	Version
libc6	2.36-9+deb12u10

File Path
/var/lib/dpkg/status.d/libc6

CVSS v3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Description

Vulnerability Namespace: debian:distro:debian:12

Vulnerability Description: GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may guess the heap addresses of pthread_created thread. The component is: glibc. NOTE: the vendor's position is "ASLR bypass itself is not a vulnerability.

Matcher: dpkg-matcher

Package URL: pkg:deb/debian/libc6@2.36-9%2Bdeb12u10?arch=arm64&distro=debian-12&upstream=glibc

References

Vulnerability Datasource: https://security-tracker.debian.org/tracker/CVE-2019-1010025

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2019-1010025

Related Vulnerability URLs:

- https://sourceware.org/bugzilla/show_bug.cgi?id=22853

- https://support.f5.com/csp/article/K06046097

- https://support.f5.com/csp/article/K06046097?utm_source=f5support&amp%3Butm_medium=RSS

- https://ubuntu.com/security/CVE-2019-1010025

- https://sourceware.org/bugzilla/show_bug.cgi?id=22853

- https://support.f5.com/csp/article/K06046097

- https://support.f5.com/csp/article/K06046097?utm_source=f5support&amp%3Butm_medium=RSS

- https://ubuntu.com/security/CVE-2019-1010025

Finding 85 - CVE-2019-9192 in libc6:2.36-9+deb12u10

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Info (7.5)	0.36% / 57.81%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['CVE-2019-9192']	72

Location

Component	Version
libc6	2.36-9+deb12u10

File Path
/var/lib/dpkg/status.d/libc6

CVSS v3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description

Vulnerability Namespace: debian:distro:debian:12

Vulnerability Description: In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/regexec.c has Uncontrolled Recursion, as demonstrated by '(|)(\1\1)' *in grep, a different issue than CVE-2018-20796. NOTE: the software maintainer disputes that this is a vulnerability because the behavior occurs only with a crafted pattern*

Matcher: dpkg-matcher

*Package URL.** pkg:deb/debian/libc6@2.36-9%2Bdeb12u10?arch=arm64&distro=debian-12&upstream=glibc

References

Vulnerability Datasource: https://security-tracker.debian.org/tracker/CVE-2019-9192

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2019-9192

Related Vulnerability URLs:

- https://sourceware.org/bugzilla/show_bug.cgi?id=24269

- https://support.f5.com/csp/article/K26346590?utm_source=f5support&amp%3Butm_medium=RSS

- https://sourceware.org/bugzilla/show_bug.cgi?id=24269

- https://support.f5.com/csp/article/K26346590?utm_source=f5support&amp%3Butm_medium=RSS

Finding 86 - CVE-2022-27943 in gcc-12-base:12.2.0-14+deb12u1

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Info (5.5)	0.05% / 15.86%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['CVE-2022-27943']	84

Location

Component	Version
gcc-12-base	12.2.0-14+deb12u1

File Path
/var/lib/dpkg/status.d/gcc-12-base

CVSS v3

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Description

Vulnerability Namespace: debian:distro:debian:12

Vulnerability Description: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as demonstrated by nm-new.

Matcher: dpkg-matcher

Package URL: pkg:deb/debian/gcc-12-base@12.2.0-14%2Bdeb12u1?arch=arm64&distro=debian-12&upstream=gcc-12

References

Vulnerability Datasource: https://security-tracker.debian.org/tracker/CVE-2022-27943

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2022-27943

Related Vulnerability URLs:

- https://gcc.gnu.org/bugzilla/show_bug.cgi?id=105039

- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/H424YXGW7OKXS2NCAP35OP6Y4P4AW6VG/

- https://sourceware.org/bugzilla/show_bug.cgi?id=28995

- https://gcc.gnu.org/bugzilla/show_bug.cgi?id=105039

- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/H424YXGW7OKXS2NCAP35OP6Y4P4AW6VG/

- https://sourceware.org/bugzilla/show_bug.cgi?id=28995

Finding 87 - CVE-2022-27943 in libgcc-s1:12.2.0-14+deb12u1

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Info (5.5)	0.05% / 15.86%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['CVE-2022-27943']	85

Location

Component	Version
libgcc-s1	12.2.0-14+deb12u1

File Path
/var/lib/dpkg/status.d/libgcc-s1

CVSS v3

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Description

Vulnerability Namespace: debian:distro:debian:12

Vulnerability Description: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as demonstrated by nm-new.

Matcher: dpkg-matcher

Package URL: pkg:deb/debian/libgcc-s1@12.2.0-14%2Bdeb12u1?arch=arm64&distro=debian-12&upstream=gcc-12

References

Vulnerability Datasource: https://security-tracker.debian.org/tracker/CVE-2022-27943

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2022-27943

Related Vulnerability URLs:

- https://gcc.gnu.org/bugzilla/show_bug.cgi?id=105039

- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/H424YXGW7OKXS2NCAP35OP6Y4P4AW6VG/

- https://sourceware.org/bugzilla/show_bug.cgi?id=28995

- https://gcc.gnu.org/bugzilla/show_bug.cgi?id=105039

- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/H424YXGW7OKXS2NCAP35OP6Y4P4AW6VG/

- https://sourceware.org/bugzilla/show_bug.cgi?id=28995

Finding 88 - CVE-2022-27943 in libgomp1:12.2.0-14+deb12u1

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Info (5.5)	0.05% / 15.86%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['CVE-2022-27943']	86

Location

Component	Version
libgomp1	12.2.0-14+deb12u1

File Path
/var/lib/dpkg/status.d/libgomp1

CVSS v3

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Description

Vulnerability Namespace: debian:distro:debian:12

Vulnerability Description: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as demonstrated by nm-new.

Matcher: dpkg-matcher

Package URL: pkg:deb/debian/libgomp1@12.2.0-14%2Bdeb12u1?arch=arm64&distro=debian-12&upstream=gcc-12

References

Vulnerability Datasource: https://security-tracker.debian.org/tracker/CVE-2022-27943

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2022-27943

Related Vulnerability URLs:

- https://gcc.gnu.org/bugzilla/show_bug.cgi?id=105039

- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/H424YXGW7OKXS2NCAP35OP6Y4P4AW6VG/

- https://sourceware.org/bugzilla/show_bug.cgi?id=28995

- https://gcc.gnu.org/bugzilla/show_bug.cgi?id=105039

- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/H424YXGW7OKXS2NCAP35OP6Y4P4AW6VG/

- https://sourceware.org/bugzilla/show_bug.cgi?id=28995

Finding 89 - CVE-2022-27943 in libstdc++6:12.2.0-14+deb12u1

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Info (5.5)	0.05% / 15.86%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['CVE-2022-27943']	87

Location

Component	Version
libstdc++6	12.2.0-14+deb12u1

File Path
/var/lib/dpkg/status.d/libstdc++6

CVSS v3

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Description

Vulnerability Namespace: debian:distro:debian:12

Vulnerability Description: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as demonstrated by nm-new.

Matcher: dpkg-matcher

Package URL: pkg:deb/debian/libstdc%2B%2B6@12.2.0-14%2Bdeb12u1?arch=arm64&distro=debian-12&upstream=gcc-12

References

Vulnerability Datasource: https://security-tracker.debian.org/tracker/CVE-2022-27943

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2022-27943

Related Vulnerability URLs:

- https://gcc.gnu.org/bugzilla/show_bug.cgi?id=105039

- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/H424YXGW7OKXS2NCAP35OP6Y4P4AW6VG/

- https://sourceware.org/bugzilla/show_bug.cgi?id=28995

- https://gcc.gnu.org/bugzilla/show_bug.cgi?id=105039

- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/H424YXGW7OKXS2NCAP35OP6Y4P4AW6VG/

- https://sourceware.org/bugzilla/show_bug.cgi?id=28995

Finding 90 - CVE-2025-27587 in libssl3:3.0.17-1~deb12u2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Vulnerability IDs	Dojo ID
Info (5.3)	0.06% / 18.35%	Active	Nov. 12, 2025	0 days	Admin User (admin)	['CVE-2025-27587']	83

Location

Component	Version
libssl3	3.0.17-1~deb12u2

File Path
/var/lib/dpkg/status.d/libssl3

CVSS v3

CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N

Description

Vulnerability Namespace: debian:distro:debian:12

Vulnerability Description: OpenSSL 3.0.0 through 3.3.2 on the PowerPC architecture is vulnerable to a Minerva attack, exploitable by measuring the time of signing of random messages using the EVP_DigestSign API, and then using the private key to extract the K value (nonce) from the signatures. Next, based on the bit size of the extracted nonce, one can compare the signing time of full-sized nonces to signatures that used smaller nonces, via statistical tests. There is a side-channel in the P-364 curve that allows private key extraction (also, there is a dependency between the bit size of K and the size of the side channel). NOTE: This CVE is disputed because the OpenSSL security policy explicitly notes that any side channels which require same physical system to be detected are outside of the threat model for the software. The timing signal is so small that it is infeasible to be detected without having the attacking process running on the same physical system.

Matcher: dpkg-matcher

Package URL: pkg:deb/debian/libssl3@3.0.17-1~deb12u2?arch=arm64&distro=debian-12&upstream=openssl

References

Vulnerability Datasource: https://security-tracker.debian.org/tracker/CVE-2025-27587

Related Vulnerability Datasource: https://nvd.nist.gov/vuln/detail/CVE-2025-27587

Related Vulnerability URLs:

- https://github.com/openssl/openssl/issues/24253

- https://minerva.crocs.fi.muni.cz