Engagement Security Report for Juice Shop

Engagement: Labs Security Testing
Generated: Nov 14, 2025

Table of Contents for Labs Security Testing

- High
  - Finding 10: CVE-2025-4802 Libc6 2.36-9+deb12u10
  - Finding 11: CVE-2018-20796 Libc6 2.36-9+deb12u10
  - Finding 12: CVE-2019-1010023 Libc6 2.36-9+deb12u10
  - Finding 13: CVE-2019-9192 Libc6 2.36-9+deb12u10
  - Finding 14: NSWG-ECO-428 Base64url 0.0.6
  - Finding 15: CVE-2024-4068 Braces 2.3.2
  - Finding 16: CVE-2020-15084 Express-JWT 0.1.3
  - Finding 17: CVE-2022-25881 HTTP-Cache-Semantics 3.8.1
  - Finding 18: CVE-2024-29415 Ip 2.0.1
  - Finding 19: CVE-2022-23539 Jsonwebtoken 0.1.0
  - Finding 20: NSWG-ECO-17 Jsonwebtoken 0.1.0
  - Finding 21: CVE-2022-23539 Jsonwebtoken 0.4.0
  - Finding 22: NSWG-ECO-17 Jsonwebtoken 0.4.0
  - Finding 23: CVE-2016-1000223 JWS 0.2.6
  - Finding 24: CVE-2021-23337 Lodash 2.4.2
  - Finding 25: CVE-2020-8203 lodash.set 4.3.2
  - Finding 26: CVE-2017-18214 Moment 2.0.0
  - Finding 27: CVE-2022-24785 Moment 2.0.0
  - Finding 28: CVE-2025-47935 Multer 1.4.5-lts.2
  - Finding 29: CVE-2025-47944 Multer 1.4.5-lts.2
  - Finding 30: CVE-2025-7338 Multer 1.4.5-lts.2
  - Finding 31: CVE-2022-25887 Sanitize-HTML 1.4.2
  - Finding 32: CVE-2024-38355 socket.io 3.1.2
  - Finding 33: CVE-2023-32695 socket.io-parser 4.0.5
  - Finding 34: CVE-2025-59343 Tar-Fs 2.1.3
  - Finding 35: CVE-2024-37890 Ws 7.4.6

- Medium
    - Finding 36: CVE-2022-27943 GCC-12-Base 12.2.0-14+deb12u1
    - Finding 37: CVE-2025-8058 Libc6 2.36-9+deb12u10
    - Finding 38: CVE-2010-4756 Libc6 2.36-9+deb12u10
    - Finding 39: CVE-2019-1010024 Libc6 2.36-9+deb12u10
    - Finding 40: CVE-2019-1010025 Libc6 2.36-9+deb12u10
    - Finding 41: CVE-2022-27943 Libgcc-S1 12.2.0-14+deb12u1
    - Finding 42: CVE-2022-27943 Libgomp1 12.2.0-14+deb12u1
    - Finding 43: CVE-2025-9230 Libssl3 3.0.17-1~deb12u2
    - Finding 44: CVE-2022-27943 Libstdc++6 12.2.0-14+deb12u1
    - Finding 45: GHSA-rvg8-pwq2-xj7q Base64url 0.0.6

- Recommendation
    - Finding 46: CVE-2022-41940 engine.io 4.1.2
    - Finding 47: CVE-2022-33987 Got 8.3.2
    - Finding 48: CVE-2022-23540 Jsonwebtoken 0.1.0
    - Finding 49: CVE-2022-23541 Jsonwebtoken 0.1.0
    - Finding 50: CVE-2022-23540 Jsonwebtoken 0.4.0
    - Finding 51: CVE-2022-23541 Jsonwebtoken 0.4.0
    - Finding 52: CVE-2018-16487 Lodash 2.4.2
    - Finding 53: CVE-2018-3721 Lodash 2.4.2
    - Finding 54: CVE-2024-4067 Micromatch 3.1.10
    - Finding 55: CVE-2016-4055 Moment 2.0.0
    - Finding 56: CVE-2025-48997 Multer 1.4.5-lts.2
    - Finding 57: CVE-2021-23771 Notevil 1.3.3
    - Finding 58: CVE-2016-1000237 Sanitize-HTML 1.4.2
    - Finding 59: CVE-2017-16016 Sanitize-HTML 1.4.2

- Finding 60: CVE-2019-25225 Sanitize-HTML 1.4.2
- Finding 61: CVE-2021-26539 Sanitize-HTML 1.4.2
- Finding 62: CVE-2021-26540 Sanitize-HTML 1.4.2
- Finding 63: CVE-2024-21501 Sanitize-HTML 1.4.2
- Finding 64: NSWG-ECO-154 Sanitize-HTML 1.4.2
- Finding 65: CVE-2024-28863 Tar 4.4.19
- Finding 66: CVE-2023-32313 Vm2 3.9.17

- Low

- Finding 67: CVE-2025-27587 Libssl3 3.0.17-1~deb12u2
- Finding 68: CVE-2025-9232 Libssl3 3.0.17-1~deb12u2
- Finding 69: CVE-2024-47764 Cookie 0.4.2
- Finding 70: CVE-2025-57349 Messageformat 2.3.0

Engagement : Labs Security Testing

Start Date	End Date	Status	Lead
Nov. 14, 2025	Nov. 14, 2026	In Progress	Admin User - Admin User (admin)

The engagement included the following tests:

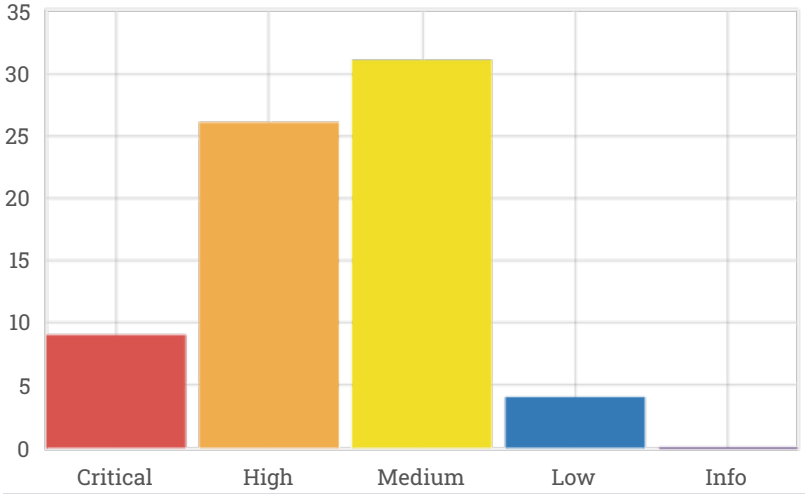
- Semgrep JSON Report (Development): 11/14/2025
- Trivy Scan (Development): 11/14/2025
- Nuclei Scan (Development): 11/14/2025
- Anchore Grype (Development): 11/14/2025

Executive Summary

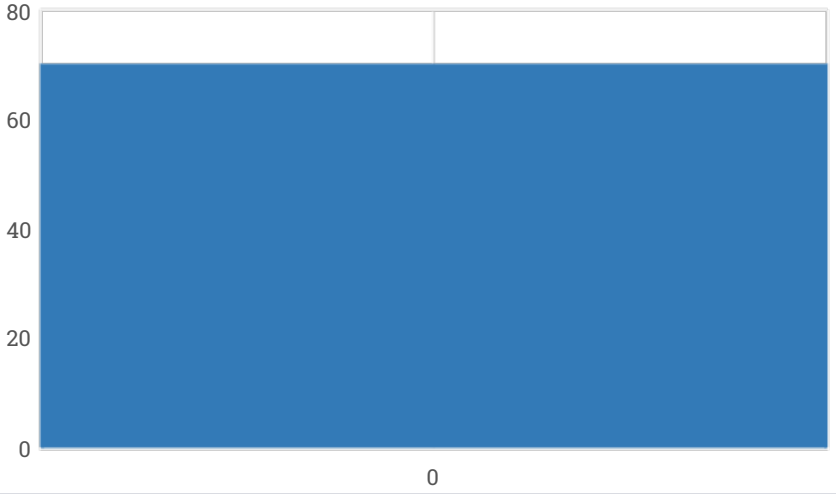
Endpoints

This report represents a security assessment performed by the Security Team team including confidential information about the state of your network and applications.
A total of 70 findings of varying severity are represented in this report.

Engagement Finding Count



Finding Age



Disclaimer

Please configure in System Settings.

Testing Notes

Findings

Critical

Finding 1: CVE-2019-1010022 Libc6 2.36-9+deb12u10

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Critical	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	119	31

Location

Component	Version
libc6	2.36-9+deb12u10

File Path
bkimminich/juice-shop:v19.0.0 (debian 12.11)

CVSS v3

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

Description

glibc: stack guard protection bypass

Target: bkimminich/juice-shop:v19.0.0 (debian 12.11)

Type: debian

Fixed version:

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.

Impact

affected

References

https://access.redhat.com/security/cve/CVE-2019-1010022

https://nvd.nist.gov/vuln/detail/CVE-2019-1010022

https://security-tracker.debian.org/tracker/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

https://www.cve.org/CVERecord?id=CVE-2019-1010022

Finding 2: CVE-2023-46233 Crypto-Js 3.3.0

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Critical	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	328	46

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

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

Target: Node.js

Type: node-pkg

Fixed version: 4.2.0

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.

Mitigation

4.2.0

Impact

fixed

References

https://access.redhat.com/security/cve/CVE-2023-46233

https://github.com/brix/crypto-js

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://nvd.nist.gov/vuln/detail/CVE-2023-46233

https://ubuntu.com/security/notices/USN-6753-1

https://www.cve.org/CVERecord?id=CVE-2023-46233

Finding 3: CVE-2015-9235 Jsonwebtoken 0.1.0

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Critical	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	20	52

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

nodejs-jsonwebtoken: verification step bypass with an altered token

Target: Node.js

Type: node-pkg

Fixed version: 4.2.2

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).

Mitigation

4.2.2

Impact

fixed

References

https://access.redhat.com/security/cve/CVE-2015-9235

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

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

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

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

https://nodesecurity.io/advisories/17

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

https://www.cve.org/CVERecord?id=CVE-2015-9235

https://www.npmjs.com/advisories/17

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

Finding 4: CVE-2015-9235 Jsonwebtoken 0.4.0

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Critical	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	20	57

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

nodejs-jsonwebtoken: verification step bypass with an altered token

Target: Node.js

Type: node-pkg

Fixed version: 4.2.2

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).

Mitigation

4.2.2

Impact

fixed

References

https://access.redhat.com/security/cve/CVE-2015-9235

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

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

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

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

https://nodesecurity.io/advisories/17

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

https://www.cve.org/CVERecord?id=CVE-2015-9235

https://www.npmjs.com/advisories/17

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

Finding 5: CVE-2019-10744 Lodash 2.4.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Critical	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	1321	63

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

nodejs-lodash: prototype pollution in defaultsDeep function leading to modifying properties

Target: Node.js

Type: node-pkg

Fixed version: 4.17.12

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.

Mitigation

4.17.12

Impact

fixed

References

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

https://access.redhat.com/security/cve/CVE-2019-10744

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

https://github.com/lodash/lodash/pull/4336

https://github.com/rubysec/ruby-advisory-db/blob/master/gems/lodash-rails/CVE-2019-10744.yml

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

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

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

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

https://support.f5.com/csp/article/K47105354

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

https://support.f5.com/csp/article/K47105354?utm_source=f5support&utm_medium=RSS

https://www.cve.org/CVERecord?id=CVE-2019-10744

https://www.npmjs.com/advisories/1065

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

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

Finding 6: GHSA-5mrr-rgp6-x4gr Marsdb 0.6.11

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Dojo ID
Critical	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	68

Location

Component	Version
marsdb	0.6.11

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

Description

Command Injection in marsdb

Target: Node.js

Type: node-pkg

Fixed version:

All versions of marsdb are vulnerable to Command Injection. In the DocumentMatcher class, selectors on $where clauses are passed to a Function constructor unsanitized. This allows attackers to run arbitrary commands in the system when the function is executed.

Recommendation

No fix is currently available. Consider using an alternative package until a fix is made available.

Impact

affected

References

https://github.com/bkimminich/juice-shop/issues/1173

https://www.npmjs.com/advisories/1122

Finding 7: CVE-2023-32314 Vm2 3.9.17

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Critical	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	74	91

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

vm2: Sandbox Escape

Target: Node.js

Type: node-pkg

Fixed version: 3.9.18

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.

Mitigation

3.9.18

Impact

fixed

References

https://access.redhat.com/security/cve/CVE-2023-32314

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

https://github.com/patriksimek/vm2

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://nvd.nist.gov/vuln/detail/CVE-2023-32314

https://www.cve.org/CVERecord?id=CVE-2023-32314

Finding 8: CVE-2023-37466 Vm2 3.9.17

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Critical	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	94	92

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

vm2: Promise handler sanitization can be bypassed allowing attackers to escape the sandbox and run arbitrary code

Target: Node.js

Type: node-pkg

Fixed version:

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.

Impact

affected

References

https://access.redhat.com/security/cve/CVE-2023-37466

https://gist.github.com/leesh3288/f693061e6523c97274ad5298eb2c74e9

https://github.com/patriksimek/vm2

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

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

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

https://www.cve.org/CVERecord?id=CVE-2023-37466

Finding 9: CVE-2023-37903 Vm2 3.9.17

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Critical	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	78	93

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

vm2: custom inspect function allows attackers to escape the sandbox and run arbitrary code

Target: Node.js

Type: node-pkg

Fixed version:

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.

Impact

affected

References

https://access.redhat.com/security/cve/CVE-2023-37903

https://github.com/patriksimek/vm2

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

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

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

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

https://www.cve.org/CVERecord?id=CVE-2023-37903

High

Finding 10: CVE-2025-4802 Libc6 2.36-9+deb12u10

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
High	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	426	27

Location

Component	Version
libc6	2.36-9+deb12u10

File Path
bkimminich/juice-shop:v19.0.0 (debian 12.11)

CVSS v3

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

Description

glibc: static setuid binary dlopen may incorrectly search LD_LIBRARY_PATH

Target: bkimminich/juice-shop:v19.0.0 (debian 12.11)

Type: debian

Fixed version: 2.36-9+deb12u11

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).

Mitigation

2.36-9+deb12u11

Impact

fixed

References

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

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

https://access.redhat.com/errata/RHSA-2025:8655

https://access.redhat.com/security/cve/CVE-2025-4802

https://bugzilla.redhat.com/2367468

https://bugzilla.redhat.com/show_bug.cgi?id=2367468

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-4802

https://errata.almalinux.org/9/ALSA-2025-8655.html

https://errata.rockylinux.org/RLSA-2025:8686

https://linux.oracle.com/cve/CVE-2025-4802.html

https://linux.oracle.com/errata/ELSA-2025-8686.html

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

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

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

https://sourceware.org/cgit/glibc/commit/?id=5451fa962cd0a90a0e2ec1d8910a559ace02bba0

https://ubuntu.com/security/notices/USN-7541-1

https://www.cve.org/CVERecord?id=CVE-2025-4802

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

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

Finding 11: CVE-2018-20796 Libc6 2.36-9+deb12u10

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
High	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	674	30

Location

Component	Version
libc6	2.36-9+deb12u10

File Path
bkimminich/juice-shop:v19.0.0 (debian 12.11)

CVSS v3

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

Description

glibc: uncontrolled recursion in function check_dst_limits_calc_pos_1 in posix/regexec.c

Target: bkimminich/juice-shop:v19.0.0 (debian 12.11)

Type: debian

Fixed version:

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.

Impact

affected

References

http://www.securityfocus.com/bid/107160

https://access.redhat.com/security/cve/CVE-2018-20796

https://debbugs.gnu.org/cgi/bugreport.cgi?bug=34141

https://lists.gnu.org/archive/html/bug-gnulib/2019-01/msg00108.html

https://nvd.nist.gov/vuln/detail/CVE-2018-20796

https://security.netapp.com/advisory/ntap-20190315-0002/

https://support.f5.com/csp/article/K26346590?utm_source=f5support&amp%3Butm_medium=RSS

https://www.cve.org/CVERecord?id=CVE-2018-20796

Finding 12: CVE-2019-1010023 Libc6 2.36-9+deb12u10

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Dojo ID
High	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	32

Location

Component	Version
libc6	2.36-9+deb12u10

File Path
bkimminich/juice-shop:v19.0.0 (debian 12.11)

CVSS v3

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

Description

glibc: running ldd on malicious ELF leads to code execution because of wrong size computation

Target: bkimminich/juice-shop:v19.0.0 (debian 12.11)

Type: debian

Fixed version:

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.

Impact

affected

References

http://www.securityfocus.com/bid/109167

https://access.redhat.com/security/cve/CVE-2019-1010023

https://nvd.nist.gov/vuln/detail/CVE-2019-1010023

https://security-tracker.debian.org/tracker/CVE-2019-1010023

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

https://www.cve.org/CVERecord?id=CVE-2019-1010023

Finding 13: CVE-2019-9192 Libc6 2.36-9+deb12u10

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
High	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	674	35

Location

Component	Version
libc6	2.36-9+deb12u10

File Path
bkimminich/juice-shop:v19.0.0 (debian 12.11)

CVSS v3

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

Description

glibc: uncontrolled recursion in function check_dst_limits_calc_pos_1 in posix/regexec.c

Target: bkimminich/juice-shop:v19.0.0 (debian 12.11)

Type: debian

Fixed version:

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

Impact

affected

References

https://access.redhat.com/security/cve/CVE-2019-9192

https://nvd.nist.gov/vuln/detail/CVE-2019-9192

https://sourceware.org/bugzilla/show_bug.cgi?id=24269

https://support.f5.com/csp/article/K26346590?utm_source=f5support&amp%3Butm_medium=RSS

https://www.cve.org/CVERecord?id=CVE-2019-9192

Finding 14: NSWG-ECO-428 Base64url 0.0.6

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Dojo ID
High	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	42

Location

Component	Version
base64url	0.0.6

File Path
juice-shop/node_modules/base64url/package.json

Description

Out-of-bounds Read

Target: Node.js

Type: node-pkg

Fixed version: >=3.0.0

base64url allocates uninitialized Buffers when number is passed in input on Node.js 4.x and below

Mitigation

=3.0.0

Impact

fixed

References

https://github.com/brianloveswords/base64url/pull/25

https://hackerone.com/reports/321687

Finding 15: CVE-2024-4068 Braces 2.3.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
High	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	1050	44

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

braces: fails to limit the number of characters it can handle

Target: Node.js

Type: node-pkg

Fixed version: 3.0.3

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.

Mitigation

3.0.3

Impact

fixed

References

https://access.redhat.com/security/cve/CVE-2024-4068

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

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

https://github.com/micromatch/braces

https://github.com/micromatch/braces/blob/98414f9f1fabe021736e26836d8306d5de747e0d/lib/parse.js#L308

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://nvd.nist.gov/vuln/detail/CVE-2024-4068

https://www.cve.org/CVERecord?id=CVE-2024-4068

Finding 16: CVE-2020-15084 Express-JWT 0.1.3

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
High	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	285	48

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

Authorization bypass in express-jwt

Target: Node.js

Type: node-pkg

Fixed version: 6.0.0

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.

Mitigation

6.0.0

Impact

fixed

References

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

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

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

Finding 17: CVE-2022-25881 HTTP-Cache-Semantics 3.8.1

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
High	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	1333	50

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

http-cache-semantics: Regular Expression Denial of Service (ReDoS) vulnerability

Target: Node.js

Type: node-pkg

Fixed version: 4.1.1

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.

Mitigation

4.1.1

Impact

fixed

References

https://access.redhat.com/errata/RHSA-2023:2655

https://access.redhat.com/security/cve/CVE-2022-25881

https://bugzilla.redhat.com/2165824

https://bugzilla.redhat.com/2168631

https://bugzilla.redhat.com/2171935

https://bugzilla.redhat.com/2172190

https://bugzilla.redhat.com/2172204

https://bugzilla.redhat.com/2172217

https://bugzilla.redhat.com/show_bug.cgi?id=2165824

https://bugzilla.redhat.com/show_bug.cgi?id=2168631

https://bugzilla.redhat.com/show_bug.cgi?id=2171935

https://bugzilla.redhat.com/show_bug.cgi?id=2172190

https://bugzilla.redhat.com/show_bug.cgi?id=2172204

https://bugzilla.redhat.com/show_bug.cgi?id=2172217

https://bugzilla.redhat.com/show_bug.cgi?id=2178076

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25881

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-4904

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23918

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23920

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23936

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24807

https://errata.almalinux.org/9/ALSA-2023-2655.html

https://errata.rockylinux.org/RLSA-2023:2655

https://github.com/kornelski/http-cache-semantics

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

https://github.com/kornelski/http-cache-semantics/commit/560b2d8ef452bbba20ffed69dc155d63ac757b74

https://linux.oracle.com/cve/CVE-2022-25881.html

https://linux.oracle.com/errata/ELSA-2023-2655.html

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

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

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://www.cve.org/CVERecord?id=CVE-2022-25881

Finding 18: CVE-2024-29415 Ip 2.0.1

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
High	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	918	51

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

node-ip: Incomplete fix for CVE-2023-42282

Target: Node.js

Type: node-pkg

Fixed version:

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.

Impact

affected

References

https://access.redhat.com/security/cve/CVE-2024-29415

https://cosmosofcyberspace.github.io/npm_ip_cve/npm_ip_cve.html

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

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://nvd.nist.gov/vuln/detail/CVE-2024-29415

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

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

https://www.cve.org/CVERecord?id=CVE-2024-29415

Finding 19: CVE-2022-23539 Jsonwebtoken 0.1.0

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
High	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	327	53

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

jsonwebtoken: Unrestricted key type could lead to legacy keys usagen

Target: Node.js

Type: node-pkg

Fixed version: 9.0.0

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.

Mitigation

9.0.0

Impact

fixed

References

https://access.redhat.com/security/cve/CVE-2022-23539

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

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

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

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

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

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

https://www.cve.org/CVERecord?id=CVE-2022-23539

Finding 20: NSWG-ECO-17 Jsonwebtoken 0.1.0

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Dojo ID
High	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	54

Location

Component	Version
jsonwebtoken	0.1.0

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

Description

Verification Bypass

Target: Node.js

Type: node-pkg

Fixed version: >=4.2.2

It is possible for an attacker to bypass verification when "a token digitally signed with an asymetric key (RS/ES family) of algorithms but instead the attacker send a token digitally signed with a symmetric algorithm (HS* family)" [1]

Mitigation

=4.2.2

Impact

fixed

References

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

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

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

Finding 21: CVE-2022-23539 Jsonwebtoken 0.4.0

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
High	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	327	58

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

jsonwebtoken: Unrestricted key type could lead to legacy keys usagen

Target: Node.js

Type: node-pkg

Fixed version: 9.0.0

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.

Mitigation

9.0.0

Impact

fixed

References

https://access.redhat.com/security/cve/CVE-2022-23539

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

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

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

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

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

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

https://www.cve.org/CVERecord?id=CVE-2022-23539

Finding 22: NSWG-ECO-17 Jsonwebtoken 0.4.0

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Dojo ID
High	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	59

Location

Component	Version
jsonwebtoken	0.4.0

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

Description

Verification Bypass

Target: Node.js

Type: node-pkg

Fixed version: >=4.2.2

It is possible for an attacker to bypass verification when "a token digitally signed with an asymetric key (RS/ES family) of algorithms but instead the attacker send a token digitally signed with a symmetric algorithm (HS* family)" [1]

Mitigation

=4.2.2

Impact

fixed

References

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

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

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

Finding 23: CVE-2016-1000223 JWS 0.2.6

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Dojo ID
High	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	62

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

Forgeable Public/Private Tokens

Target: Node.js

Type: node-pkg

Fixed version: >=3.0.0

Since "algorithm" isn't enforced in jws.verify(), a malicious user could choose what algorithm is sent to the server. If the server is expecting RSA but is sent HMAC-SHA with RSA's public key, the server will think the public key is actually an HMAC private key. This could be used to forge any data an attacker wants.

In addition, there is the none algorithm to be concerned about. In versions prior to 3.0.0, verification of the token could be bypassed when the alg field is set to none.

Edit (7/29/16): A previous version of this advisory incorrectly stated that the vulnerability was patched in version 2.0.0 instead of 3.0.0. The advisory has been updated to reflect this new information. Thanks to Fabien Catteau for reporting the error.

Mitigation

=3.0.0

Impact

fixed

References

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

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

https://github.com/brianloveswords/node-jws

https://github.com/brianloveswords/node-jws/commit/585d0e1e97b6747c10cf5b7689ccc5618a89b299#diff-4ac32a78649ca5bdd8e0ba38b7006a1e

https://nvd.nist.gov/vuln/detail/CVE-2016-1000223

https://snyk.io/vuln/npm:jws:20160726

https://www.npmjs.com/advisories/88

Finding 24: CVE-2021-23337 Lodash 2.4.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
High	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	94	65

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

nodejs-lodash: command injection via template

Target: Node.js

Type: node-pkg

Fixed version: 4.17.21

Lodash versions prior to 4.17.21 are vulnerable to Command Injection via the template function.

Mitigation

4.17.21

Impact

fixed

References

https://access.redhat.com/security/cve/CVE-2021-23337

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

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

https://github.com/lodash/lodash

https://github.com/lodash/lodash/blob/ddfd9b11a0126db2302cb70ec9973b66baec0975/lodash.js

https://github.com/lodash/lodash/blob/ddfd9b11a0126db2302cb70ec9973b66baec0975/lodash.js#L14851

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

https://github.com/lodash/lodash/commit/3469357cff396a26c363f8c1b5a91dde28ba4b1c

https://github.com/rubysec/ruby-advisory-db/blob/master/gems/lodash-rails/CVE-2021-23337.yml

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

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

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.cve.org/CVERecord?id=CVE-2021-23337

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 25: CVE-2020-8203 lodash.set 4.3.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
High	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	770	67

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

nodejs-lodash: prototype pollution in zipObjectDeep function

Target: Node.js

Type: node-pkg

Fixed version:

Prototype pollution attack when using _.zipObjectDeep in lodash before 4.17.20.

Impact

affected

References

https://access.redhat.com/security/cve/CVE-2020-8203

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

https://github.com/github/advisory-database/pull/2884

https://github.com/lodash/lodash

https://github.com/lodash/lodash/commit/c84fe82760fb2d3e03a63379b297a1cc1a2fce12

https://github.com/lodash/lodash/issues/4744

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

https://github.com/lodash/lodash/wiki/Changelog#v41719

https://github.com/rubysec/ruby-advisory-db/blob/master/gems/lodash-rails/CVE-2020-8203.yml

https://hackerone.com/reports/712065

https://hackerone.com/reports/864701

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

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

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

https://web.archive.org/web/20210914001339/https://github.com/lodash/lodash/issues/4744

https://www.cve.org/CVERecord?id=CVE-2020-8203

https://www.npmjs.com/advisories/1523

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 26: CVE-2017-18214 Moment 2.0.0

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
High	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	400	71

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

nodejs-moment: Regular expression denial of service

Target: Node.js

Type: node-pkg

Fixed version: 2.19.3

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.

Mitigation

2.19.3

Impact

fixed

References

https://access.redhat.com/security/cve/CVE-2017-18214

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

https://github.com/moment/moment

https://github.com/moment/moment/commit/69ed9d44957fa6ab12b73d2ae29d286a857b80eb

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

https://github.com/moment/moment/pull/4326

https://nodesecurity.io/advisories/532

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

https://ubuntu.com/security/notices/USN-4786-1

https://www.cve.org/CVERecord?id=CVE-2017-18214

https://www.npmjs.com/advisories/532

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

Finding 27: CVE-2022-24785 Moment 2.0.0

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
High	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	22	72

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

Moment.js: Path traversal in moment.locale

Target: Node.js

Type: node-pkg

Fixed version: 2.29.2

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.

Mitigation

2.29.2

Impact

fixed

References

https://access.redhat.com/security/cve/CVE-2022-24785

https://github.com/moment/moment

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://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/6QIO6YNLTK2T7SPKDS4JEL45FANLNC2Q

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

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

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

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

https://ubuntu.com/security/notices/USN-5559-1

https://www.cve.org/CVERecord?id=CVE-2022-24785

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

Finding 28: CVE-2025-47935 Multer 1.4.5-lts.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
High	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	401	74

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

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

Target: Node.js

Type: node-pkg

Fixed version: 2.0.0

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.

Mitigation

2.0.0

Impact

fixed

References

https://github.com/expressjs/multer

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

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

Finding 29: CVE-2025-47944 Multer 1.4.5-lts.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
High	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	248	75

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

Multer vulnerable to Denial of Service from maliciously crafted requests

Target: Node.js

Type: node-pkg

Fixed version: 2.0.0

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.

Mitigation

2.0.0

Impact

fixed

References

https://github.com/expressjs/multer

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

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

Finding 30: CVE-2025-7338 Multer 1.4.5-lts.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
High	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	248	77

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

multer: Multer Denial of Service

Target: Node.js

Type: node-pkg

Fixed version: 2.0.2

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.

Mitigation

2.0.2

Impact

fixed

References

https://access.redhat.com/security/cve/CVE-2025-7338

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

https://github.com/expressjs/multer

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

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

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

https://www.cve.org/CVERecord?id=CVE-2025-7338

Finding 31: CVE-2022-25887 Sanitize-HTML 1.4.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
High	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	1333	79

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

sanitize-html: insecure global regular expression replacement logic may lead to ReDoS

Target: Node.js

Type: node-pkg

Fixed version: 2.7.1

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.

Mitigation

2.7.1

Impact

fixed

References

https://access.redhat.com/security/cve/CVE-2022-25887

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

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

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

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

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

https://ubuntu.com/security/notices/USN-7464-1

https://www.cve.org/CVERecord?id=CVE-2022-25887

Finding 32: CVE-2024-38355 socket.io 3.1.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
High	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	20	87

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

socket.io: Unhandled 'error' event

Target: Node.js

Type: node-pkg

Fixed version: 2.5.1, 4.6.2

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.

Mitigation

2.5.1, 4.6.2

Impact

fixed

References

https://access.redhat.com/security/cve/CVE-2024-38355

https://github.com/socketio/socket.io

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://nvd.nist.gov/vuln/detail/CVE-2024-38355

https://www.cve.org/CVERecord?id=CVE-2024-38355

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

Finding 33: CVE-2023-32695 socket.io-parser 4.0.5

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
High	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	20	88

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

socket.io parser is a socket.io encoder and decoder written in JavaScr ...

Target: Node.js

Type: node-pkg

Fixed version: 4.2.3, 3.4.3, 3.3.4

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.

Mitigation

4.2.3, 3.4.3, 3.3.4

Impact

fixed

References

https://github.com/socketio/socket.io-parser

https://github.com/socketio/socket.io-parser/commit/1c220ddbf45ea4b44bc8dbf6f9ae245f672ba1b9

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/commit/ee006607495eca4ec7262ad080dd3a91439a5ba4

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://nvd.nist.gov/vuln/detail/CVE-2023-32695

Finding 34: CVE-2025-59343 Tar-Fs 2.1.3

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
High	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	22	90

Location

Component	Version
tar-fs	2.1.3

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

CVSS v3

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

Description

tar-fs: tar-fs symlink validation bypass

Target: Node.js

Type: node-pkg

Fixed version: 3.1.1, 2.1.4, 1.16.6

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.

Mitigation

3.1.1, 2.1.4, 1.16.6

Impact

fixed

References

https://access.redhat.com/security/cve/CVE-2025-59343

https://github.com/mafintosh/tar-fs

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

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

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

https://www.cve.org/CVERecord?id=CVE-2025-59343

Finding 35: CVE-2024-37890 Ws 7.4.6

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
High	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	476	95

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

nodejs-ws: denial of service when handling a request with many HTTP headers

Target: Node.js

Type: node-pkg

Fixed version: 5.2.4, 6.2.3, 7.5.10, 8.17.1

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.

Mitigation

5.2.4, 6.2.3, 7.5.10, 8.17.1

Impact

fixed

References

https://access.redhat.com/security/cve/CVE-2024-37890

https://github.com/websockets/ws

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://nvd.nist.gov/vuln/detail/CVE-2024-37890

https://www.cve.org/CVERecord?id=CVE-2024-37890

Medium

Finding 36: CVE-2022-27943 GCC-12-Base 12.2.0-14+deb12u1

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	674	26

Location

Component	Version
gcc-12-base	12.2.0-14+deb12u1

File Path
bkimminich/juice-shop:v19.0.0 (debian 12.11)

CVSS v3

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

Description

binutils: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack exhaustion in demangle_const

Target: bkimminich/juice-shop:v19.0.0 (debian 12.11)

Type: debian

Fixed version:

libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as demonstrated by nm-new.

Impact

affected

References

https://access.redhat.com/security/cve/CVE-2022-27943

https://gcc.gnu.org/bugzilla/show_bug.cgi?id=105039

https://gcc.gnu.org/git/gitweb.cgi?p=gcc.git;h=1a770b01ef415e114164b6151d1e55acdee09371

https://gcc.gnu.org/git/gitweb.cgi?p=gcc.git;h=9234cdca6ee88badfc00297e72f13dac4e540c79

https://gcc.gnu.org/git/gitweb.cgi?p=gcc.git;h=fc968115a742d9e4674d9725ce9c2106b91b6ead

https://gcc.gnu.org/pipermail/gcc-patches/2022-March/592244.html

https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/H424YXGW7OKXS2NCAP35OP6Y4P4AW6VG/

https://nvd.nist.gov/vuln/detail/CVE-2022-27943

https://sourceware.org/bugzilla/show_bug.cgi?id=28995

https://www.cve.org/CVERecord?id=CVE-2022-27943

Finding 37: CVE-2025-8058 Libc6 2.36-9+deb12u10

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	415	28

Location

Component	Version
libc6	2.36-9+deb12u10

File Path
bkimminich/juice-shop:v19.0.0 (debian 12.11)

CVSS v3

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

Description

glibc: Double free in glibc

Target: bkimminich/juice-shop:v19.0.0 (debian 12.11)

Type: debian

Fixed version: 2.36-9+deb12u13

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.

Mitigation

2.36-9+deb12u13

Impact

fixed

References

https://access.redhat.com/errata/RHSA-2025:12980

https://access.redhat.com/security/cve/CVE-2025-8058

https://bugzilla.redhat.com/2383146

https://bugzilla.redhat.com/show_bug.cgi?id=2383146

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-8058

https://errata.almalinux.org/8/ALSA-2025-12980.html

https://errata.rockylinux.org/RLSA-2025:12980

https://linux.oracle.com/cve/CVE-2025-8058.html

https://linux.oracle.com/errata/ELSA-2025-20595.html

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

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

https://sourceware.org/git/?p=glibc.git;a=blob_plain;f=advisories/GLIBC-SA-2025-0005

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

https://ubuntu.com/security/notices/USN-7760-1

https://www.cve.org/CVERecord?id=CVE-2025-8058

Finding 38: CVE-2010-4756 Libc6 2.36-9+deb12u10

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	399	29

Location

Component	Version
libc6	2.36-9+deb12u10

File Path
bkimminich/juice-shop:v19.0.0 (debian 12.11)

Description

glibc: glob implementation can cause excessive CPU and memory consumption due to crafted glob expressions

Target: bkimminich/juice-shop:v19.0.0 (debian 12.11)

Type: debian

Fixed version:

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.

Impact

affected

References

http://cxib.net/stuff/glob-0day.c

http://securityreason.com/achievement_securityalert/89

http://securityreason.com/exploitalert/9223

https://access.redhat.com/security/cve/CVE-2010-4756

https://bugzilla.redhat.com/show_bug.cgi?id=681681

https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2010-4756

https://nvd.nist.gov/vuln/detail/CVE-2010-4756

https://www.cve.org/CVERecord?id=CVE-2010-4756

Finding 39: CVE-2019-1010024 Libc6 2.36-9+deb12u10

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	200	33

Location

Component	Version
libc6	2.36-9+deb12u10

File Path
bkimminich/juice-shop:v19.0.0 (debian 12.11)

CVSS v3

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

Description

glibc: ASLR bypass using cache of thread stack and heap

Target: bkimminich/juice-shop:v19.0.0 (debian 12.11)

Type: debian

Fixed version:

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.

Impact

affected

References

http://www.securityfocus.com/bid/109162

https://access.redhat.com/security/cve/CVE-2019-1010024

https://nvd.nist.gov/vuln/detail/CVE-2019-1010024

https://security-tracker.debian.org/tracker/CVE-2019-1010024

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

https://www.cve.org/CVERecord?id=CVE-2019-1010024

Finding 40: CVE-2019-1010025 Libc6 2.36-9+deb12u10

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	330	34

Location

Component	Version
libc6	2.36-9+deb12u10

File Path
bkimminich/juice-shop:v19.0.0 (debian 12.11)

CVSS v3

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

Description

glibc: information disclosure of heap addresses of pthread_created thread

Target: bkimminich/juice-shop:v19.0.0 (debian 12.11)

Type: debian

Fixed version:

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.

Impact

affected

References

https://access.redhat.com/security/cve/CVE-2019-1010025

https://nvd.nist.gov/vuln/detail/CVE-2019-1010025

https://security-tracker.debian.org/tracker/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

https://www.cve.org/CVERecord?id=CVE-2019-1010025

Finding 41: CVE-2022-27943 Libgcc-S1 12.2.0-14+deb12u1

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	674	36

Location

Component	Version
libgcc-s1	12.2.0-14+deb12u1

File Path
bkimminich/juice-shop:v19.0.0 (debian 12.11)

CVSS v3

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

Description

binutils: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack exhaustion in demangle_const

Target: bkimminich/juice-shop:v19.0.0 (debian 12.11)

Type: debian

Fixed version:

libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as demonstrated by nm-new.

Impact

affected

References

https://access.redhat.com/security/cve/CVE-2022-27943

https://gcc.gnu.org/bugzilla/show_bug.cgi?id=105039

https://gcc.gnu.org/git/gitweb.cgi?p=gcc.git;h=1a770b01ef415e114164b6151d1e55acdee09371

https://gcc.gnu.org/git/gitweb.cgi?p=gcc.git;h=9234cdca6ee88badfc00297e72f13dac4e540c79

https://gcc.gnu.org/git/gitweb.cgi?p=gcc.git;h=fc968115a742d9e4674d9725ce9c2106b91b6ead

https://gcc.gnu.org/pipermail/gcc-patches/2022-March/592244.html

https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/H424YXGW7OKXS2NCAP35OP6Y4P4AW6VG/

https://nvd.nist.gov/vuln/detail/CVE-2022-27943

https://sourceware.org/bugzilla/show_bug.cgi?id=28995

https://www.cve.org/CVERecord?id=CVE-2022-27943

Finding 42: CVE-2022-27943 Libgomp1 12.2.0-14+deb12u1

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	674	37

Location

Component	Version
libgomp1	12.2.0-14+deb12u1

File Path
bkimminich/juice-shop:v19.0.0 (debian 12.11)

CVSS v3

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

Description

binutils: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack exhaustion in demangle_const

Target: bkimminich/juice-shop:v19.0.0 (debian 12.11)

Type: debian

Fixed version:

libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as demonstrated by nm-new.

Impact

affected

References

https://access.redhat.com/security/cve/CVE-2022-27943

https://gcc.gnu.org/bugzilla/show_bug.cgi?id=105039

https://gcc.gnu.org/git/gitweb.cgi?p=gcc.git;h=1a770b01ef415e114164b6151d1e55acdee09371

https://gcc.gnu.org/git/gitweb.cgi?p=gcc.git;h=9234cdca6ee88badfc00297e72f13dac4e540c79

https://gcc.gnu.org/git/gitweb.cgi?p=gcc.git;h=fc968115a742d9e4674d9725ce9c2106b91b6ead

https://gcc.gnu.org/pipermail/gcc-patches/2022-March/592244.html

https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/H424YXGW7OKXS2NCAP35OP6Y4P4AW6VG/

https://nvd.nist.gov/vuln/detail/CVE-2022-27943

https://sourceware.org/bugzilla/show_bug.cgi?id=28995

https://www.cve.org/CVERecord?id=CVE-2022-27943

Finding 43: CVE-2025-9230 Libssl3 3.0.17-1~deb12u2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	125	38

Location

Component	Version
libssl3	3.0.17-1~deb12u2

File Path
bkimminich/juice-shop:v19.0.0 (debian 12.11)

CVSS v3

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

Description

openssl: Out-of-bounds read & write in RFC 3211 KEK Unwrap

Target: bkimminich/juice-shop:v19.0.0 (debian 12.11)

Type: debian

Fixed version: 3.0.17-1~deb12u3

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.

Mitigation

3.0.17-1~deb12u3

Impact

fixed

References

https://access.redhat.com/security/cve/CVE-2025-9230

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://nvd.nist.gov/vuln/detail/CVE-2025-9230

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

https://ubuntu.com/security/notices/USN-7786-1

https://www.cve.org/CVERecord?id=CVE-2025-9230

Finding 44: CVE-2022-27943 Libstdc++6 12.2.0-14+deb12u1

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	674	41

Location

Component	Version
libstdc++6	12.2.0-14+deb12u1

File Path
bkimminich/juice-shop:v19.0.0 (debian 12.11)

CVSS v3

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

Description

binutils: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack exhaustion in demangle_const

Target: bkimminich/juice-shop:v19.0.0 (debian 12.11)

Type: debian

Fixed version:

libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as demonstrated by nm-new.

Impact

affected

References

https://access.redhat.com/security/cve/CVE-2022-27943

https://gcc.gnu.org/bugzilla/show_bug.cgi?id=105039

https://gcc.gnu.org/git/gitweb.cgi?p=gcc.git;h=1a770b01ef415e114164b6151d1e55acdee09371

https://gcc.gnu.org/git/gitweb.cgi?p=gcc.git;h=9234cdca6ee88badfc00297e72f13dac4e540c79

https://gcc.gnu.org/git/gitweb.cgi?p=gcc.git;h=fc968115a742d9e4674d9725ce9c2106b91b6ead

https://gcc.gnu.org/pipermail/gcc-patches/2022-March/592244.html

https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/H424YXGW7OKXS2NCAP35OP6Y4P4AW6VG/

https://nvd.nist.gov/vuln/detail/CVE-2022-27943

https://sourceware.org/bugzilla/show_bug.cgi?id=28995

https://www.cve.org/CVERecord?id=CVE-2022-27943

Finding 45: GHSA-rvg8-pwq2-xj7q Base64url 0.0.6

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Dojo ID
Medium	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	43

Location	
Component	**Version**
base64url	0.0.6

File Path
juice-shop/node_modules/base64url/package.json

Description

Out-of-bounds Read in base64url

Target: Node.js

Type: node-pkg

Fixed version: 3.0.0

Versions of base64url before 3.0.0 are vulnerable to to out-of-bounds reads as it allocates uninitialized Buffers when number is passed in input on Node.js 4.x and below.

Recommendation

Update to version 3.0.0 or later.

Mitigation

3.0.0

Impact

fixed

References

https://github.com/brianloveswords/base64url

https://github.com/brianloveswords/base64url/commit/4fbd954a0a69e9d898de2146557cc6e893e79542

https://github.com/brianloveswords/base64url/pull/25

https://hackerone.com/reports/321687

Finding 46: CVE-2022-41940 engine.io 4.1.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	248	47

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

engine.io: Specially crafted HTTP request can trigger an uncaught exception

Target: Node.js

Type: node-pkg

Fixed version: 3.6.1, 6.2.1

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.

Mitigation

3.6.1, 6.2.1

Impact

fixed

References

https://access.redhat.com/security/cve/CVE-2022-41940

https://github.com/socketio/engine.io

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://nvd.nist.gov/vuln/detail/CVE-2022-41940

https://www.cve.org/CVERecord?id=CVE-2022-41940

Finding 47: CVE-2022-33987 Got 8.3.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Dojo ID
Medium	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	49

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

nodejs-got: missing verification of requested URLs allows redirects to UNIX sockets

Target: Node.js

Type: node-pkg

Fixed version: 12.1.0, 11.8.5

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

Mitigation

12.1.0, 11.8.5

Impact

fixed

References

https://access.redhat.com/errata/RHSA-2022:6595

https://access.redhat.com/security/cve/CVE-2022-33987

https://bugzilla.redhat.com/1907444

https://bugzilla.redhat.com/1945459

https://bugzilla.redhat.com/1964461

https://bugzilla.redhat.com/2007557

https://bugzilla.redhat.com/2098556

https://bugzilla.redhat.com/2102001

https://bugzilla.redhat.com/2105422

https://bugzilla.redhat.com/2105426

https://bugzilla.redhat.com/2105428

https://bugzilla.redhat.com/2105430

https://errata.almalinux.org/9/ALSA-2022-6595.html

https://github.com/sindresorhus/got

https://github.com/sindresorhus/got/commit/861ccd9ac2237df762a9e2beed7edd88c60782dc

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/releases/tag/v12.1.0

https://linux.oracle.com/cve/CVE-2022-33987.html

https://linux.oracle.com/errata/ELSA-2022-6595.html

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

https://www.cve.org/CVERecord?id=CVE-2022-33987

Finding 48: CVE-2022-23540 Jsonwebtoken 0.1.0

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	287	55

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

jsonwebtoken: Insecure default algorithm in jwt.verify() could lead to signature validation bypass

Target: Node.js

Type: node-pkg

Fixed version: 9.0.0

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.

Mitigation

9.0.0

Impact

fixed

References

https://access.redhat.com/security/cve/CVE-2022-23540

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

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

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

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

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

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

https://www.cve.org/CVERecord?id=CVE-2022-23540

Finding 49: CVE-2022-23541 Jsonwebtoken 0.1.0

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	287	56

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

jsonwebtoken: Insecure implementation of key retrieval function could lead to Forgeable Public/Private Tokens from RSA to HMAC

Target: Node.js

Type: node-pkg

Fixed version: 9.0.0

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.

Mitigation

9.0.0

Impact

fixed

References

https://access.redhat.com/security/cve/CVE-2022-23541

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

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://nvd.nist.gov/vuln/detail/CVE-2022-23541

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

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

https://www.cve.org/CVERecord?id=CVE-2022-23541

Finding 50: CVE-2022-23540 Jsonwebtoken 0.4.0

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	287	60

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

jsonwebtoken: Insecure default algorithm in jwt.verify() could lead to signature validation bypass

Target: Node.js

Type: node-pkg

Fixed version: 9.0.0

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.

Mitigation

9.0.0

Impact

fixed

References

https://access.redhat.com/security/cve/CVE-2022-23540

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

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

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

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

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

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

https://www.cve.org/CVERecord?id=CVE-2022-23540

Finding 51: CVE-2022-23541 Jsonwebtoken 0.4.0

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	287	61

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

jsonwebtoken: Insecure implementation of key retrieval function could lead to Forgeable Public/Private Tokens from RSA to HMAC

Target: Node.js

Type: node-pkg

Fixed version: 9.0.0

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.

Mitigation

9.0.0

Impact

fixed

References

https://access.redhat.com/security/cve/CVE-2022-23541

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

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://nvd.nist.gov/vuln/detail/CVE-2022-23541

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

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

https://www.cve.org/CVERecord?id=CVE-2022-23541

Finding 52: CVE-2018-16487 Lodash 2.4.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	400	64

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

lodash: Prototype pollution in utilities function

Target: Node.js

Type: node-pkg

Fixed version: >=4.17.11

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.

Mitigation

=4.17.11

Impact

fixed

References

https://access.redhat.com/security/cve/CVE-2018-16487

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

https://github.com/lodash/lodash/commit/90e6199a161b6445b01454517b40ef65ebecd2ad

https://github.com/rubysec/ruby-advisory-db/blob/master/gems/lodash-rails/CVE-2018-16487.yml

https://hackerone.com/reports/380873

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

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

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

https://www.cve.org/CVERecord?id=CVE-2018-16487

https://www.npmjs.com/advisories/782

Finding 53: CVE-2018-3721 Lodash 2.4.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	471	66

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

lodash: Prototype pollution in utilities function

Target: Node.js

Type: node-pkg

Fixed version: >=4.17.5

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.

Mitigation

=4.17.5

Impact

fixed

References

https://access.redhat.com/security/cve/CVE-2018-3721

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

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

https://github.com/rubysec/ruby-advisory-db/blob/master/gems/lodash-rails/CVE-2018-3721.yml

https://hackerone.com/reports/310443

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

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

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

https://snyk.io/vuln/npm:lodash:20180130

https://www.cve.org/CVERecord?id=CVE-2018-3721

https://www.npmjs.com/advisories/577

Finding 54: CVE-2024-4067 Micromatch 3.1.10

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	1333	70

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

micromatch: vulnerable to Regular Expression Denial of Service

Target: Node.js

Type: node-pkg

Fixed version: 4.0.8

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.

Mitigation

4.0.8

Impact

fixed

References

https://access.redhat.com/security/cve/CVE-2024-4067

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

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

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

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

https://github.com/micromatch/micromatch

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

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

https://github.com/micromatch/micromatch/commit/500d5d6f42f0e8dfa1cb5464c6cb420b1b6aaaa0

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

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

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

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

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

https://www.cve.org/CVERecord?id=CVE-2024-4067

Finding 55: CVE-2016-4055 Moment 2.0.0

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	400	73

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:L/UI:N/S:U/C:N/I:N/A:H

Description

moment.js: regular expression denial of service

Target: Node.js

Type: node-pkg

Fixed version: >=2.11.2

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)."

Mitigation

=2.11.2

Impact

fixed

References

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://access.redhat.com/security/cve/CVE-2016-4055

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

https://github.com/moment/moment

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

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

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

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

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

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

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

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

https://nodesecurity.io/advisories/55

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

https://ubuntu.com/security/notices/USN-4786-1

https://www.cve.org/CVERecord?id=CVE-2016-4055

https://www.npmjs.com/advisories/55

https://www.owasp.org/index.php/Regular_expression_Denial_of_Service_-_ReDoS

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

Finding 56: CVE-2025-48997 Multer 1.4.5-lts.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	248	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:L

Description

multer: Multer vulnerable to Denial of Service via unhandled exception

Target: Node.js

Type: node-pkg

Fixed version: 2.0.1

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.

Mitigation

2.0.1

Impact

fixed

References

https://access.redhat.com/security/cve/CVE-2025-48997

https://github.com/expressjs/multer

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

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

https://www.cve.org/CVERecord?id=CVE-2025-48997

Finding 57: CVE-2021-23771 Notevil 1.3.3

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	1321	78

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

Sandbox escape in notevil and argencoders-notevil

Target: Node.js

Type: node-pkg

Fixed version:

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.

Impact

affected

References

https://github.com/mmckegg/notevil

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

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

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

Finding 58: CVE-2016-1000237 Sanitize-HTML 1.4.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	79	80

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

XSS - Sanitization not applied recursively

Target: Node.js

Type: node-pkg

Fixed version: >=1.4.3

sanitize-html before 1.4.3 has XSS.

Mitigation

=1.4.3

Impact

fixed

References

https://github.com/apostrophecms/sanitize-html/commit/762fbc7bba389f3f789cc291c1eb2b64f60f2caf

https://github.com/apostrophecms/sanitize-html/issues/29

https://github.com/punkave/sanitize-html/issues/29

https://nodesecurity.io/advisories/135

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

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

https://www.npmjs.com/advisories/135

Finding 59: CVE-2017-16016 Sanitize-HTML 1.4.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	79	81

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

Cross-Site Scripting in sanitize-html

Target: Node.js

Type: node-pkg

Fixed version: 1.11.4

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.

Mitigation

1.11.4

Impact

fixed

References

https://github.com/advisories/GHSA-xc6g-ggrc-qq4r

https://github.com/punkave/sanitize-html/commit/5d205a1005ba0df80e21d8c64a15bb3accdb2403

https://github.com/punkave/sanitize-html/commit/5d205a1005ba0df80e21d8c64a15bb3accdb2403)))

https://github.com/punkave/sanitize-html/issues/100

https://nodesecurity.io/advisories/154

https://npmjs.com/package/sanitize-html#discarding-the-entire-contents-of-a-disallowed-tag

https://nvd.nist.gov/vuln/detail/CVE-2017-16016

https://www.npmjs.com/advisories/154

Finding 60: CVE-2019-25225 Sanitize-HTML 1.4.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	79	82

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

sanitize-html: sanitize-html cross site scripting

Target: Node.js

Type: node-pkg

Fixed version: 2.0.0-beta

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.

Mitigation

2.0.0-beta

Impact

fixed

References

https://access.redhat.com/security/cve/CVE-2019-25225

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

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

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

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

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

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

https://www.cve.org/CVERecord?id=CVE-2019-25225

Finding 61: CVE-2021-26539 Sanitize-HTML 1.4.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Dojo ID
Medium	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	83

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

sanitize-html: improper handling of internationalized domain name (IDN) can lead to bypass hostname whitelist validation

Target: Node.js

Type: node-pkg

Fixed version: 2.3.1

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.

Mitigation

2.3.1

Impact

fixed

References

https://access.redhat.com/security/cve/CVE-2021-26539

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

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

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

https://github.com/apostrophecms/sanitize-html/commit/bdf7836ef8f0e5b21f9a1aab0623ae8fcd09c1da

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

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

https://www.cve.org/CVERecord?id=CVE-2021-26539

Finding 62: CVE-2021-26540 Sanitize-HTML 1.4.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Dojo ID
Medium	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	84

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

sanitize-html: improper validation of hostnames set by the "allowedIframeHostnames" option can lead to bypass hostname whitelist for iframe element

Target: Node.js

Type: node-pkg

Fixed version: 2.3.2

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".

Mitigation

2.3.2

Impact

fixed

References

https://access.redhat.com/security/cve/CVE-2021-26540

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://nvd.nist.gov/vuln/detail/CVE-2021-26540

https://www.cve.org/CVERecord?id=CVE-2021-26540

Finding 63: CVE-2024-21501 Sanitize-HTML 1.4.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	200	85

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

sanitize-html: Information Exposure when used on the backend

Target: Node.js

Type: node-pkg

Fixed version: 2.12.1

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.

Mitigation

2.12.1

Impact

fixed

References

https://access.redhat.com/security/cve/CVE-2024-21501

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

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

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

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/4EB5JPYRCTS64EA5AMV3INHDPI6I4AW7/

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

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

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

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

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

https://www.cve.org/CVERecord?id=CVE-2024-21501

Finding 64: NSWG-ECO-154 Sanitize-HTML 1.4.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	Dojo ID
Medium	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	86

Location

Component	Version
sanitize-html	1.4.2

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

Description

Cross Site Scripting

Target: Node.js

Type: node-pkg

Fixed version: >=1.11.4

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.

PoC:

```
var sanitizeHtml = require('sanitize-html');

var dirty = '!<textarea>&lt;/textarea&gt;<svg/onload=prompt`xs`&gt;</textarea>!';
var clean = sanitizeHtml(dirty, {
   allowedTags: [ 'textarea' ]
});

console.log(clean);

// !<textarea></textarea><svg/onload=prompt`xs`></textarea>!
```

Mitigation

=1.11.4

Impact

fixed

References

https://github.com/punkave/sanitize-html/commit/5d205a1005ba0df80e21d8c64a15bb3accdb2403

https://github.com/punkave/sanitize-html/issues/100

Finding 65: CVE-2024-28863 Tar 4.4.19

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	400	89

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

node-tar: denial of service while parsing a tar file due to lack of folders depth validation

Target: Node.js

Type: node-pkg

Fixed version: 6.2.1

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.

Mitigation

6.2.1

Impact

fixed

References

https://access.redhat.com/errata/RHSA-2024:6147

https://access.redhat.com/security/cve/CVE-2024-28863

https://bugzilla.redhat.com/2293200

https://bugzilla.redhat.com/2296417

https://errata.almalinux.org/9/ALSA-2024-6147.html

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

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

https://github.com/isaacs/node-tar/commit/fe8cd57da5686f8695415414bda49206a545f7f7 (v6.2.1)

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

https://linux.oracle.com/cve/CVE-2024-28863.html

https://linux.oracle.com/errata/ELSA-2024-6148.html

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

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

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

https://www.cve.org/CVERecord?id=CVE-2024-28863

Finding 66: CVE-2023-32313 Vm2 3.9.17

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Medium	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	74	94

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

vm2: Inspect Manipulation

Target: Node.js

Type: node-pkg

Fixed version: 3.9.18

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.

Mitigation

3.9.18

Impact

fixed

References

https://access.redhat.com/security/cve/CVE-2023-32313

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

https://github.com/patriksimek/vm2

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://nvd.nist.gov/vuln/detail/CVE-2023-32313

https://www.cve.org/CVERecord?id=CVE-2023-32313

Low

Finding 67: CVE-2025-27587 Libssl3 3.0.17-1~deb12u2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Low	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	385	39

Location

Component	Version
libssl3	3.0.17-1~deb12u2

File Path
bkimminich/juice-shop:v19.0.0 (debian 12.11)

Description

OpenSSL 3.0.0 through 3.3.2 on the PowerPC architecture is vulnerable ...

Target: bkimminich/juice-shop:v19.0.0 (debian 12.11)

Type: debian

Fixed version:

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.

Impact

affected

References

https://github.com/openssl/openssl/issues/24253

https://minerva.crocs.fi.muni.cz

https://www.cve.org/CVERecord?id=CVE-2025-27587

Finding 68: CVE-2025-9232 Libssl3 3.0.17-1~deb12u2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Low	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	125	40

Location

Component	Version
libssl3	3.0.17-1~deb12u2

File Path
bkimminich/juice-shop:v19.0.0 (debian 12.11)

CVSS v3

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

Description

openssl: Out-of-bounds read in HTTP client no_proxy handling

Target: bkimminich/juice-shop:v19.0.0 (debian 12.11)

Type: debian

Fixed version: 3.0.17-1~deb12u3

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.

Mitigation

3.0.17-1~deb12u3

Impact

fixed

References

https://access.redhat.com/security/cve/CVE-2025-9232

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://nvd.nist.gov/vuln/detail/CVE-2025-9232

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

https://ubuntu.com/security/notices/USN-7786-1

https://www.cve.org/CVERecord?id=CVE-2025-9232

Finding 69: CVE-2024-47764 Cookie 0.4.2

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Low	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	74	45

Location

Component	Version
cookie	0.4.2

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

CVSS v3

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

Description

cookie: cookie accepts cookie name, path, and domain with out of bounds characters

Target: Node.js

Type: node-pkg

Fixed version: 0.7.0

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.

Mitigation

0.7.0

Impact

fixed

References

https://access.redhat.com/security/cve/CVE-2024-47764

https://github.com/jshttp/cookie

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

https://nvd.nist.gov/vuln/detail/CVE-2024-47764

https://www.cve.org/CVERecord?id=CVE-2024-47764

Finding 70: CVE-2025-57349 Messageformat 2.3.0

Severity	EPSS Score / Percentile	Status	Date discovered	Age	Reporter	CWE	Dojo ID
Low	N.A. / N.A.	Active, Verified	Nov. 14, 2025	0 days	Admin User (admin)	1321	69

Location

Component	Version
messageformat	2.3.0

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

Description

messageformat has a prototype pollution vulnerability

Target: Node.js

Type: node-pkg

Fixed version: 3.0.0-beta.0

The messageformat package, an implementation of the Unicode MessageFormat 2 specification for JavaScript, is vulnerable to prototype pollution due to improper handling of message key paths in versions prior to 2.3.0. The flaw arises when processing nested message keys containing special characters (e.g., **proto**), which can lead to unintended modification of the JavaScript Object prototype. This vulnerability may allow a remote attacker to inject properties into the global object prototype via specially crafted message input, potentially causing denial of service or other undefined behaviors in applications using the affected component.

Mitigation

3.0.0-beta.0

Impact

fixed

References

https://github.com/messageformat/messageformat

https://github.com/messageformat/messageformat/issues/452

https://nvd.nist.gov/vuln/detail/CVE-2025-57349