nodegoat: Findings

Client: Demo client · **Prepared by:** Unvarnish demo · **Generated:** 2026-11-14 10:11 UTC
Source: repo `https://github.com/OWASP/NodeGoat.git` at `c5cb68a7084e`

> Produced by Unvarnish's deterministic scanners. Every finding below is reproducible and traceable to a file and line. Model-assisted analysis was not run for this document.

Executive summary

No model-written text for this section: no model configured.

Summary

164 finding(s): 34 critical, 86 high, 37 medium, 7 low.

120 finding(s) are critical or high severity and need action before this tool is relied on further.

By the numbers

Measure	Value
Files analysed / total	92 / 111
Source lines	4,956
Largest source file	`app/views/tutorial/a1.html` (409 lines)
Longest source function	`SessionHandler` in `app/routes/session.js` (268 lines)
Languages (source lines)	html 2,933; javascript 2,005; dockerfile 18
Frameworks	Express
Automated tests	present
Secrets (current / history only)	6 / 19
Client-exposed credentials / open tables	0 / 0
Dependencies declared	36
Dependency vulnerabilities	311 (33 critical, 170 high, 94 medium, 14 low)

Measure	Value
End-of-life runtimes and frameworks	1 past end of life, 0 near it; endoflife.date data dated 2026-11-14
Hardcoded infrastructure	33 URLs · 0 internal host(s) · 1 IP(s) · 0 path(s) · 0 email(s)
Commits · authors · active days	499 · 40 · 204
History span	2013-10-21 to 2023-06-21
Top author share · bus factor	49% · 2
Commits over 2,000 lines	7
AI tooling indicators	none found

Largest source files

File	Lines	Longest function
`app/views/tutorial/a1.html`	409	—
`app/views/tutorial/a2.html`	310	—
`app/routes/session.js`	277	`SessionHandler` (268)
`app/views/tutorial/a3.html`	243	—
`Gruntfile.js`	194	`<anonymous>` (181)

Remediation outlook

Findings by remediation effort: S up to half a day, M up to two days, L up to a week, XL weeks. Scanner findings carry a fixed band per rule; model findings carry the model's band, adjusted by the verifier where it checked the finding. The bands are an input to the consultant's judgment, not a quote.

Severity	S	M	L	XL	Not estimated	Total
critical	34	0	0	0	0	34
high	66	19	1	0	0	86
medium	31	4	2	0	0	37
low	7	0	0	0	0	7
Total	138	23	3	0	0	164

Findings

Critical (34)

Private key material

`security` · source: scanner (secrets) · effort: S · id `7a8c5a682b3ae372`

Private key material found in artifacts/cert/server.key. The value is redacted here and identified by fingerprint.

Impact. Anyone who can read this code or its history holds a working credential. Rotation is required regardless of whether the file is still present.

Remediation. Rotate the credential now. Move it to a secret manager or environment variable. Purge it from git history (git filter-repo) before the repository moves anywhere.

Effort. S: rotate one credential and move it to configuration (scanner rule secrets.credential)

Evidence.

- `artifacts/cert/server.key:1` — `…[redacted 31 chars]` (fingerprint 71960cee9226; also appears in 1 commit(s) in git history)

Hardcoded credential assignment

`security` · source: scanner (secrets) · effort: S · id `e962539144197d1e`

Hardcoded credential assignment found in artifacts/db-reset.js. The value is redacted here and identified by fingerprint.

Impact. Anyone who can read this code or its history holds a working credential. Rotation is required regardless of whether the file is still present.

Remediation. Rotate the credential now. Move it to a secret manager or environment variable. Purge it from git history (git filter-repo) before the repository moves anywhere.

Effort. S: rotate one credential and move it to configuration (scanner rule secrets.credential)

Evidence.

- `artifacts/db-reset.js:18` — `"password": "…[redacted 9 chars]",` (fingerprint d07e7c4cce2a; also appears in 2 commit(s) in git history)

Hardcoded credential assignment

`security` · source: scanner (secrets) · effort: S · id `3946d6a7836769cb`

Hardcoded credential assignment found in artifacts/db-reset.js (1 more occurrence(s) with the same value). The value is redacted here and identified by fingerprint.

Impact. Anyone who can read this code or its history holds a working credential. Rotation is required regardless of whether the file is still present.

Remediation. Rotate the credential now. Move it to a secret manager or environment variable. Purge it from git history (git filter-repo) before the repository moves anywhere.

Effort. S: rotate one credential and move it to configuration (scanner rule secrets.credential)

Evidence.

- `artifacts/db-reset.js:27` — `"password": "…[redacted 9 chars]"` (fingerprint b4ea3116d868; also appears in 4 commit(s) in git history)

Hardcoded credential assignment

`security` · source: scanner (secrets) · effort: S · id `6fb3798154516a9f`

Hardcoded credential assignment found in artifacts/db-reset.js. The value is redacted here and identified by fingerprint.

Impact. Anyone who can read this code or its history holds a working credential. Rotation is required regardless of whether the file is still present.

Remediation. Rotate the credential now. Move it to a secret manager or environment variable. Purge it from git history (git filter-repo) before the repository moves anywhere.

Effort. S: rotate one credential and move it to configuration (scanner rule secrets.credential)

Evidence.

- `artifacts/db-reset.js:35` — `"password": "…[redacted 9 chars]"` (fingerprint 5238f6fe78d6; also appears in 2 commit(s) in git history)

Hardcoded credential assignment

`security` · source: scanner (secrets) · effort: S · id `45d4acc332770fb7`

Hardcoded credential assignment found in config/env/all.js. The value is redacted here and identified by fingerprint.

Impact. Anyone who can read this code or its history holds a working credential. Rotation is required regardless of whether the file is still present.

Remediation. Rotate the credential now. Move it to a secret manager or environment variable. Purge it from git history (git filter-repo) before the repository moves anywhere.

Effort. S: rotate one credential and move it to configuration (scanner rule secrets.credential)

Evidence.

- `config/env/all.js:8` — `cookieSecret: "…[redacted 30 chars]",` (fingerprint 6f983a53bf8b; also appears in 1 commit(s) in git history)

Hardcoded credential assignment

`security` · source: scanner (secrets) · effort: S · id `f5a688cb1a6b4647`

Hardcoded credential assignment found in config/env/development.js (1 more occurrence(s) with the same value). The value is redacted here and identified by fingerprint.

Impact. Anyone who can read this code or its history holds a working credential. Rotation is required regardless of whether the file is still present.

Remediation. Rotate the credential now. Move it to a secret manager or environment variable. Purge it from git history (git filter-repo) before the repository moves anywhere.

Effort. S: rotate one credential and move it to configuration (scanner rule secrets.credential)

Evidence.

- `config/env/development.js:6` — `zapApiKey: "…[redacted 26 chars]",` (fingerprint e0f1906c2cc8; also appears in 3 commit(s) in git history)

Known vulnerabilities in babel-traverse 6.11.4

`dependency` · source: scanner (dependencies) · effort: S · id `b6c24dac5b455885`

1 published advisory affects babel-traverse 6.11.4 (npm), declared in package-lock.json: GHSA-67hx-6×53-jw92: Babel vulnerable to arbitrary code execution when compiling specifically crafted malicious code.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade babel-traverse to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-67hx-6×53-jw92)

Known vulnerabilities in bson 1.0.9

`dependency` · source: scanner (dependencies) · effort: S · id `afc17a71947119f5`

2 published advisories affect bson 1.0.9 (npm), declared in package-lock.json: GHSA-4jwp-vfvf-657p: Deserialization of Untrusted Data in bson; GHSA-v8w9-2789-6hhr: Deserialization of Untrusted Data in bson.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade bson to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-4jwp-vfvf-657p, GHSA-v8w9-2789-6hhr)

Known vulnerabilities in form-data 0.1.4

`dependency` · source: scanner (dependencies) · effort: S · id `fc4e3bf311868841`

2 published advisories affect form-data 0.1.4 (npm), declared in package-lock.json: GHSA-fjxv-7rqg-78g4: form-data uses unsafe random function in form-data for choosing boundary; GHSA-hmw2-7cc7-3qxx: form-data: CRLF injection in form-data via unescaped multipart field names and filenames.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade form-data to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-fjxv-7rqg-78g4, GHSA-hmw2-7cc7-3qxx)

Known vulnerabilities in form-data 1.0.1

`dependency` · source: scanner (dependencies) · effort: S · id `43a89b1479b45f2e`

2 published advisories affect form-data 1.0.1 (npm), declared in package-lock.json: GHSA-fjxv-7rqg-78g4: form-data uses unsafe random function in form-data for choosing boundary; GHSA-hmw2-7cc7-3qxx: form-data: CRLF injection in form-data via unescaped multipart field names and filenames.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade form-data to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-fjxv-7rqg-78g4, GHSA-hmw2-7cc7-3qxx)

Known vulnerabilities in form-data 2.0.0

`dependency` · source: scanner (dependencies) · effort: S · id `26234cf19a4c0382`

2 published advisories affect form-data 2.0.0 (npm), declared in package-lock.json: GHSA-fjxv-7rqg-78g4: form-data uses unsafe random function in form-data for choosing boundary; GHSA-hmw2-7cc7-3qxx: form-data: CRLF injection in form-data via unescaped multipart field names and filenames.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade form-data to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-fjxv-7rqg-78g4, GHSA-hmw2-7cc7-3qxx)

Known vulnerabilities in form-data 2.1.4

`dependency` · source: scanner (dependencies) · effort: S · id `539cf36b66b4d6ed`

2 published advisories affect form-data 2.1.4 (npm), declared in package-lock.json: GHSA-fjxv-7rqg-78g4: form-data uses unsafe random function in form-data for choosing boundary; GHSA-hmw2-7cc7-3qxx: form-data: CRLF injection in form-data via unescaped multipart field names and filenames.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade form-data to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-fjxv-7rqg-78g4, GHSA-hmw2-7cc7-3qxx)

Known vulnerabilities in form-data 2.3.3

`dependency` · source: scanner (dependencies) · effort: S · id `ad345d6814cb3fe8`

2 published advisories affect form-data 2.3.3 (npm), declared in package-lock.json: GHSA-fjxv-7rqg-78g4: form-data uses unsafe random function in form-data for choosing boundary; GHSA-hmw2-7cc7-3qxx: form-data: CRLF injection in form-data via unescaped multipart field names and filenames.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade form-data to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-fjxv-7rqg-78g4, GHSA-hmw2-7cc7-3qxx)

Known vulnerabilities in fsevents 1.2.9

`dependency` · source: scanner (dependencies) · effort: S · id `f967f58c918b082c`

2 published advisories affect fsevents 1.2.9 (npm), declared in package-lock.json: MAL-2023-462: Malicious code in fsevents (npm); GHSA-8r6j-v8pm-fqw3: Code injection in fsevents.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade fsevents to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: MAL-2023-462, GHSA-8r6j-v8pm-fqw3)

Known vulnerabilities in getobject 0.1.0

`dependency` · source: scanner (dependencies) · effort: S · id `d1a35feef651fdd7`

1 published advisory affects getobject 0.1.0 (npm), declared in package-lock.json: GHSA-957j-59c2-j692: Prototype pollution in getobject.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade getobject to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-957j-59c2-j692)

Known vulnerabilities in growl 1.9.2

`dependency` · source: scanner (dependencies) · effort: S · id `5fde59f3fa1ae98b`

1 published advisory affects growl 1.9.2 (npm), declared in package-lock.json: GHSA-qh2h-chj9-jffq: Growl before 1.10.0 vulnerable to Command Injection.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade growl to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-qh2h-chj9-jffq)

Known vulnerabilities in handlebars 4.0.5

`dependency` · source: scanner (dependencies) · effort: S · id `7a3976a6c82cfef4`

20 published advisories affect handlebars 4.0.5 (npm), declared in package-lock.json: GHSA-2cf5-4w76-r9qv: Arbitrary Code Execution in handlebars; GHSA-2qvq-rjwj-gvw9: Handlebars.js has Prototype Pollution Leading to XSS through Partial Template Injection; GHSA-2w6w-674q-4c4q: Handlebars.js has JavaScript Injection via AST Type Confusion; GHSA-3cqr-58rm-57f8: Arbitrary Code Execution in Handlebars; GHSA-3mfm-83xf-c92r: Handlebars.js has JavaScript Injection via AST Type Confusion by tampering @partial-block; GHSA-442j-39wm-28r2: Handlebars.js has a Property Access Validation Bypass in container.lookup; GHSA-62gr-4qp9-h98f: Regular Expression Denial of Service in Handlebars; GHSA-765h-qjxv-5f44: Prototype Pollution in handlebars; GHSA-8r5x-fm3f-whwj: Handlebars: JavaScript Injection via AST Type Confusion in compile (bypass of CVE-2026-33937); GHSA-9cx6-37pm-9jff: Handlebars.js has Denial of Service via Malformed Decorator Syntax in Template Compilation; and 10 more.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade handlebars to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-2cf5-4w76-r9qv, GHSA-2qvq-rjwj-gvw9, GHSA-2w6w-674q-4c4q, GHSA-3cqr-58rm-57f8, GHSA-3mfm-83xf-c92r, GHSA-442j-39wm-28r2, GHSA-62gr-4qp9-h98f, GHSA-765h-qjxv-5f44, GHSA-8r5x-fm3f-whwj, GHSA-9cx6-37pm-9jff, GHSA-f2jv-r9rf-7988, GHSA-f52g-6jhx-586p, GHSA-g9r4-xpmj-mj65, GHSA-p8wg-vrv2-v86f, GHSA-q2c6-c6pm-g3gh, GHSA-q42p-pg8m-cqh6, GHSA-w457-6q6x-cgp9, GHSA-xhpv-hc6g-r9c6, GHSA-xjpj-3mr7-gcpf, GHSA-xw65-4hp5-5hc7)

Known vulnerabilities in json-schema 0.2.3

`dependency` · source: scanner (dependencies) · effort: S · id `8f5f29e64a44e2f3`

1 published advisory affects json-schema 0.2.3 (npm), declared in package-lock.json: GHSA-896r-f27r-55mw: json-schema is vulnerable to Prototype Pollution.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade json-schema to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-896r-f27r-55mw)

Known vulnerabilities in lodash 2.4.2

`dependency` · source: scanner (dependencies) · effort: S · id `6ba969185e8e5c1e`

4 published advisories affect lodash 2.4.2 (npm), declared in package-lock.json: GHSA-35jh-r3h4-6jhm: Command Injection in lodash; GHSA-4xc9-xhrj-v574: Prototype Pollution in lodash; GHSA-fvqr-27wr-82fm: Prototype Pollution in lodash; GHSA-jf85-cpcp-j695: Prototype Pollution in lodash.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade lodash to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-35jh-r3h4-6jhm, GHSA-4xc9-xhrj-v574, GHSA-fvqr-27wr-82fm, GHSA-jf85-cpcp-j695)

Known vulnerabilities in lodash 4.13.1

`dependency` · source: scanner (dependencies) · effort: S · id `606d74f135e303f2`

9 published advisories affect lodash 4.13.1 (npm), declared in package-lock.json: GHSA-29mw-wpgm-hmr9: Regular Expression Denial of Service (ReDoS) in lodash; GHSA-35jh-r3h4-6jhm: Command Injection in lodash; GHSA-4xc9-xhrj-v574: Prototype Pollution in lodash; GHSA-fvqr-27wr-82fm: Prototype Pollution in lodash; GHSA-jf85-cpcp-j695: Prototype Pollution in lodash; GHSA-p6mc-m468-83gw: Prototype Pollution in lodash; GHSA-r5fr-rjxr-66jc: lodash vulnerable to Code Injection via `_.template` imports key names; GHSA-x5rq-j2xg-h7qm: Regular Expression Denial of Service (ReDoS) in lodash; GHSA-xxjr-mmjv-4gpg: Lodash has Prototype Pollution Vulnerability in `_.unset`, `_.omit`, and `_.pullAt` functions.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade lodash to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-29mw-wpgm-hmr9, GHSA-35jh-r3h4-6jhm, GHSA-4xc9-xhrj-v574, GHSA-fvqr-27wr-82fm, GHSA-jf85-cpcp-j695, GHSA-p6mc-m468-83gw, GHSA-r5fr-rjxr-66jc, GHSA-x5rq-j2xg-h7qm, GHSA-xxjr-mmjv-4gpg)

Known vulnerabilities in lodash 4.17.11

`dependency` · source: scanner (dependencies) · effort: S · id `3f06bf820dc28010`

6 published advisories affect lodash 4.17.11 (npm), declared in package-lock.json: GHSA-29mw-wpgm-hmr9: Regular Expression Denial of Service (ReDoS) in lodash; GHSA-35jh-r3h4-6jhm: Command Injection in lodash; GHSA-jf85-cpcp-j695: Prototype Pollution in lodash; GHSA-p6mc-m468-83gw: Prototype Pollution in lodash; GHSA-r5fr-rjxr-66jc: lodash vulnerable to Code Injection via `_.template` imports key names; GHSA-xxjr-mmjv-4gpg: Lodash has Prototype Pollution Vulnerability in `_.unset`, `_.omit`, and `_.pullAt` functions.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade lodash to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-29mw-wpgm-hmr9, GHSA-35jh-r3h4-6jhm, GHSA-jf85-cpcp-j695, GHSA-p6mc-m468-83gw, GHSA-r5fr-rjxr-66jc, GHSA-xxjr-mmjv-4gpg)

Known vulnerabilities in minimist 0.0.10

`dependency` · source: scanner (dependencies) · effort: S · id `fd868e83e7290e02`

2 published advisories affect minimist 0.0.10 (npm), declared in package-lock.json: GHSA-vh95-rmgr-6w4m: Prototype Pollution in minimist; GHSA-xvch-5gv4-984h: Prototype Pollution in minimist.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade minimist to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-vh95-rmgr-6w4m, GHSA-xvch-5gv4-984h)

Known vulnerabilities in minimist 0.0.8

`dependency` · source: scanner (dependencies) · effort: S · id `cb39b8dc834eb586`

2 published advisories affect minimist 0.0.8 (npm), declared in package-lock.json: GHSA-vh95-rmgr-6w4m: Prototype Pollution in minimist; GHSA-xvch-5gv4-984h: Prototype Pollution in minimist.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade minimist to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-vh95-rmgr-6w4m, GHSA-xvch-5gv4-984h)

Known vulnerabilities in minimist 1.2.0

`dependency` · source: scanner (dependencies) · effort: S · id `bf09d326abae8672`

2 published advisories affect minimist 1.2.0 (npm), declared in package-lock.json: GHSA-vh95-rmgr-6w4m: Prototype Pollution in minimist; GHSA-xvch-5gv4-984h: Prototype Pollution in minimist.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade minimist to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-vh95-rmgr-6w4m, GHSA-xvch-5gv4-984h)

Known vulnerabilities in minimist 1.2.5

`dependency` · source: scanner (dependencies) · effort: S · id `8e86189ec470bb22`

1 published advisory affects minimist 1.2.5 (npm), declared in package-lock.json: GHSA-xvch-5gv4-984h: Prototype Pollution in minimist.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade minimist to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-xvch-5gv4-984h)

Known vulnerabilities in mixin-deep 1.3.1

`dependency` · source: scanner (dependencies) · effort: S · id `71e1f797b1f8d742`

1 published advisory affects mixin-deep 1.3.1 (npm), declared in package-lock.json: GHSA-fhjf-83wg-r2j9: Prototype Pollution in mixin-deep.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade mixin-deep to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-fhjf-83wg-r2j9)

Known vulnerabilities in proxy-addr 2.0.4

`dependency` · source: scanner (dependencies) · effort: S · id `1b7e2fbb1a03ea95`

1 published advisory affects proxy-addr 2.0.4 (npm), declared in package-lock.json: GHSA-jqcg-44mw-7w3h: proxy-addr vulnerable to IP spoofing via IPv4-mapped IPv6 trust subnet.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade proxy-addr to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-jqcg-44mw-7w3h)

Known vulnerabilities in set-value 0.4.3

`dependency` · source: scanner (dependencies) · effort: S · id `7f4aa7dd858a9ca9`

2 published advisories affect set-value 0.4.3 (npm), declared in package-lock.json: GHSA-4g88-fppr-53pp: Prototype Pollution in set-value; GHSA-4jqc-8m5r-9rpr: Prototype Pollution in set-value.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade set-value to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-4g88-fppr-53pp, GHSA-4jqc-8m5r-9rpr)

Known vulnerabilities in set-value 2.0.0

`dependency` · source: scanner (dependencies) · effort: S · id `9585f6fc3fbfb5a3`

2 published advisories affect set-value 2.0.0 (npm), declared in package-lock.json: GHSA-4g88-fppr-53pp: Prototype Pollution in set-value; GHSA-4jqc-8m5r-9rpr: Prototype Pollution in set-value.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade set-value to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-4g88-fppr-53pp, GHSA-4jqc-8m5r-9rpr)

Known vulnerabilities in tar 2.2.1

`dependency` · source: scanner (dependencies) · effort: S · id `a70252fc6085fc3f`

16 published advisories affect tar 2.2.1 (npm), declared in package-lock.json: GHSA-23hp-3jrh-7fpw: node-tar: Decompression/parse DoS via unlimited input; GHSA-34×7-hfp2-rc4v: node-tar Vulnerable to Arbitrary File Creation/Overwrite via Hardlink Path Traversal; GHSA-3jfq-g458-7qm9: Arbitrary File Creation/Overwrite due to insufficient absolute path sanitization; GHSA-5955-9wpr-37jh: Arbitrary File Creation/Overwrite on Windows via insufficient relative path sanitization; GHSA-83g3-92jg-28cx: Arbitrary File Read/Write via Hardlink Target Escape Through Symlink Chain in node-tar Extraction; GHSA-8qq5-rm4j-mr97: node-tar is Vulnerable to Arbitrary File Overwrite and Symlink Poisoning via Insufficient Path Sanitization; GHSA-8×88-c5mf-7j5w: node-tar: Negative tar entry size causes infinite loop in archive replace; GHSA-9ppj-qmqm-q256: node-tar Symlink Path Traversal via Drive-Relative Linkpath; GHSA-f5×3-32g6-xq36: Denial of service while parsing a tar file due to lack of folders count validation; GHSA-gvwx-54wh-qm9j: node-tar: Uncaught Exception DoS via NUL byte in PAX path/linkpath records; and 6 more.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade tar to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-23hp-3jrh-7fpw, GHSA-34×7-hfp2-rc4v, GHSA-3jfq-g458-7qm9, GHSA-5955-9wpr-37jh, GHSA-83g3-92jg-28cx, GHSA-8qq5-rm4j-mr97, GHSA-8×88-c5mf-7j5w, GHSA-9ppj-qmqm-q256, GHSA-f5×3-32g6-xq36, GHSA-gvwx-54wh-qm9j, GHSA-j44m-qm6p-hp7m, GHSA-qffp-2rhf-9h96, GHSA-r292-9mhp-454m, GHSA-r6q2-hw4h-h46w, GHSA-vmf3-w455-68vh, GHSA-w8wr-v893-vjvp)

Known vulnerabilities in tar 4.4.8

`dependency` · source: scanner (dependencies) · effort: S · id `0879c74681cb1c9c`

18 published advisories affect tar 4.4.8 (npm), declared in package-lock.json: GHSA-23hp-3jrh-7fpw: node-tar: Decompression/parse DoS via unlimited input; GHSA-34×7-hfp2-rc4v: node-tar Vulnerable to Arbitrary File Creation/Overwrite via Hardlink Path Traversal; GHSA-3jfq-g458-7qm9: Arbitrary File Creation/Overwrite due to insufficient absolute path sanitization; GHSA-5955-9wpr-37jh: Arbitrary File Creation/Overwrite on Windows via insufficient relative path sanitization; GHSA-83g3-92jg-28cx: Arbitrary File Read/Write via Hardlink Target Escape Through Symlink Chain in node-tar Extraction; GHSA-8qq5-rm4j-mr97: node-tar is Vulnerable to Arbitrary File Overwrite and Symlink Poisoning via Insufficient Path Sanitization; GHSA-8×88-c5mf-7j5w: node-tar: Negative tar entry size causes infinite loop in archive replace; GHSA-9ppj-qmqm-q256: node-tar Symlink Path Traversal via Drive-Relative Linkpath; GHSA-9r2w-394v-53qc: Arbitrary File

Creation/Overwrite via insufficient symlink protection due to directory cache poisoning using symbolic links; GHSA-f5×3-32g6-xq36: Denial of service while parsing a tar file due to lack of folders count validation; and 8 more.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade tar to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-23hp-3jrh-7fpw, GHSA-34×7-hfp2-rc4v, GHSA-3jfq-g458-7qm9, GHSA-5955-9wpr-37jh, GHSA-83g3-92jg-28cx, GHSA-8qq5-rm4j-mr97, GHSA-8×88-c5mf-7j5w, GHSA-9ppj-qmqm-q256, GHSA-9r2w-394v-53qc, GHSA-f5×3-32g6-xq36, GHSA-gvwx-54wh-qm9j, GHSA-qffp-2rhf-9h96, GHSA-qq89-hq3f-393p, GHSA-r292-9mhp-454m, GHSA-r628-mhmh-qjhw, GHSA-r6q2-hw4h-h46w, GHSA-vmf3-w455-68vh, GHSA-w8wr-v893-vjvp)

Known vulnerabilities in underscore 1.8.3

`dependency` · source: scanner (dependencies) · effort: S · id `e8b9de56dc109a15`

2 published advisories affect underscore 1.8.3 (npm), declared in package-lock.json: GHSA-cf4h-3jhx-xvhq: Arbitrary Code Execution in underscore; GHSA-qpx9-hpmf-5gmw: Underscore has unlimited recursion in _.flatten and _.isEqual, potential for DoS attack.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade underscore to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-cf4h-3jhx-xvhq, GHSA-qpx9-hpmf-5gmw)

Known vulnerabilities in underscore 1.9.1

`dependency` · source: scanner (dependencies) · effort: S · id `c358505f77d59702`

2 published advisories affect underscore 1.9.1 (npm), declared in package-lock.json: GHSA-cf4h-3jhx-xvhq: Arbitrary Code Execution in underscore; GHSA-qpx9-hpmf-5gmw: Underscore has unlimited recursion in _.flatten and _.isEqual, potential for DoS attack.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade underscore to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-cf4h-3jhx-xvhq, GHSA-qpx9-hpmf-5gmw)

Known vulnerabilities in websocket-driver 0.7.0

`dependency` · source: scanner (dependencies) · effort: S · id `b0155bffd9b3fe46`

2 published advisories affect websocket-driver 0.7.0 (npm), declared in package-lock.json: GHSA-mp7j-qc5w-4988: websocket-driver: Resource limit bypass via message compression; GHSA-xv26-6w52-cph6: websocket-driver: Message corruption via abuse of protocol length headers.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade websocket-driver to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-mp7j-qc5w-4988, GHSA-xv26-6w52-cph6)

High (86)

Node.js 12 is past end of life

`dependency` · source: scanner (end_of_life) · effort: L · id `ad1e243c348a1c96`

Node.js 12 reached end of life on 2022-04-30: its maintainers no longer fix bugs or security issues in it. It is declared in Dockerfile. Dates are from endoflife.date data dated 2026-11-14.

Impact. Security flaws found from now on in this release are not fixed upstream, so the tool accumulates known vulnerabilities, and libraries drop support for it, which blocks routine upgrades.

Remediation. Move to a release its maintainers still support, test the tool on it, and update every place listed below. Supported releases include Node.js 26.

Effort. L: move to a supported release, retest and update every place it is pinned (scanner rule end_of_life.past)

Evidence.

- `Dockerfile:1` (FROM node:12-alpine; end of life 2022-04-30; endoflife.date data dated 2026-11-14)
- `Dockerfile:7` (FROM node:12-alpine; end of life 2022-04-30; endoflife.date data dated 2026-11-14)

Private key material in git history

`security` · source: scanner (secrets) · effort: M · id `d769b326f2760eec`

Private key material found in app/cert/key.pem. The value is redacted here and identified by fingerprint.

Impact. Anyone who can read this code or its history holds a working credential. Rotation is required regardless of whether the file is still present.

Remediation. Rotate the credential now. Move it to a secret manager or environment variable. Purge it from git history (git filter-repo) before the repository moves anywhere.

Effort. M: rotate the credential, then rewrite history every clone must take (scanner rule secrets.credential_history)

Evidence.

- `app/cert/key.pem` — `…[redacted 31 chars]` (fingerprint e21ad48d54bf; added in commit e0045e653a53; removed from the working tree but recoverable by anyone with repository access)

Database connection string with embedded password in git history

`security` · source: scanner (secrets) · effort: M · id `0c31573952184c10`

Database connection string with embedded password found in config/env/all.js. The value is redacted here and identified by fingerprint.

Impact. Anyone who can read this code or its history holds a working credential. Rotation is required regardless of whether the file is still present.

Remediation. Rotate the credential now. Move it to a secret manager or environment variable. Purge it from git history (git filter-repo) before the repository moves anywhere.

Effort. M: rotate the credential, then rewrite history every clone must take (scanner rule secrets.credential_history)

Evidence.

- `config/env/all.js` — `db = process.env.NODE_ENV === 'test' ? 'mongodb://localhost:27017/nodegoat' : 'mongodb://nodegoat:…[redacted 5 chars]@nodegoat-cluster-shard-00-00.zkkl5.mongodb.net:27017,nodegoat-cluster-shard-00-01.` (fingerprint 1ec32ca39b42; added in commit 5ab008832d7e; removed from the working tree but recoverable by anyone with repository access)

Private key material in git history

`security` · source: scanner (secrets) · effort: M · id `4078eebdcde2c323`

Private key material found in node_modules/forever/node_modules/cliff/node_modules/winston/node_modules/request/tests/ssl/ca/ca.key. The value is redacted here and identified by fingerprint.

Impact. Anyone who can read this code or its history holds a working credential. Rotation is required regardless of whether the file is still present.

Remediation. Rotate the credential now. Move it to a secret manager or environment variable. Purge it from git history (git filter-repo) before the repository moves anywhere.

Effort. M: rotate the credential, then rewrite history every clone must take (scanner rule secrets.credential_history)

Evidence.

- `node_modules/forever/node_modules/cliff/node_modules/winston/node_modules/request/tests/ssl/ca/ca.key` — `…[redacted 31 chars]` (fingerprint de6c258eed0a; added in commit a7b556da2a25; removed from the working tree but recoverable by anyone with repository access)

Private key material in git history

`security` · source: scanner (secrets) · effort: M · id `0767acc3b195dc75`

Private key material found in node_modules/forever/node_modules/cliff/node_modules/winston/node_modules/request/tests/ssl/ca/server.key. The value is redacted here and identified by fingerprint.

Impact. Anyone who can read this code or its history holds a working credential. Rotation is required regardless of whether the file is still present.

Remediation. Rotate the credential now. Move it to a secret manager or environment variable. Purge it from git history (git filter-repo) before the repository moves anywhere.

Effort. M: rotate the credential, then rewrite history every clone must take (scanner rule secrets.credential_history)

Evidence.

- `node_modules/forever/node_modules/cliff/node_modules/winston/node_modules/request/tests/ssl/ca/server.key` — `…[redacted 31 chars]` (fingerprint e5ad552764bc; added in commit a7b556da2a25; removed from the working tree but recoverable by anyone with repository access)

Private key material in git history

`security` · source: scanner (secrets) · effort: M · id `03e773dbd1cd310c`

Private key material found in node_modules/forever/node_modules/cliff/node_modules/winston/node_modules/request/tests/ssl/test.key. The value is redacted here and identified by fingerprint.

Impact. Anyone who can read this code or its history holds a working credential. Rotation is required regardless of whether the file is still present.

Remediation. Rotate the credential now. Move it to a secret manager or environment variable. Purge it from git history (git filter-repo) before the repository moves anywhere.

Effort. M: rotate the credential, then rewrite history every clone must take (scanner rule secrets.credential_history)

Evidence.

- `node_modules/forever/node_modules/cliff/node_modules/winston/node_modules/request/tests/ssl/test.key` — `…[redacted 31 chars]` (fingerprint adbcb67e3a6c; added in commit a7b556da2a25; removed from the working tree but recoverable by anyone with repository access)

Hardcoded credential assignment in git history

`security` · source: scanner (secrets) · effort: M · id `9601ed3b9a94f745`

Hardcoded credential assignment found in node_modules/forever/node_modules/cliff/node_modules/winston/node_modules/request/tests/test-oauth.js. The value is redacted here and identified by fingerprint.

Impact. Anyone who can read this code or its history holds a working credential. Rotation is required regardless of whether the file is still present.

Remediation. Rotate the credential now. Move it to a secret manager or environment variable. Purge it from git history (git filter-repo) before the repository moves anywhere.

Effort. M: rotate the credential, then rewrite history every clone must take (scanner rule secrets.credential_history)

Evidence.

- `node_modules/forever/node_modules/cliff/node_modules/winston/node_modules/request/tests/test-oauth.js` — `, oauth_token: '…[redacted 41 chars]'` (fingerprint 46804ea1cd86; added in commit a7b556da2a25; removed from the working tree but recoverable by anyone with repository access)

Hardcoded credential assignment in git history

`security` · source: scanner (secrets) · effort: M · id `b7db9ce0b7219c54`

Hardcoded credential assignment found in node_modules/forever/node_modules/cliff/node_modules/winston/node_modules/request/tests/test-oauth.js. The value is redacted here and identified by fingerprint.

Impact. Anyone who can read this code or its history holds a working credential. Rotation is required regardless of whether the file is still present.

Remediation. Rotate the credential now. Move it to a secret manager or environment variable. Purge it from git history (git filter-repo) before the repository moves anywhere.

Effort. M: rotate the credential, then rewrite history every clone must take (scanner rule secrets.credential_history)

Evidence.

- `node_modules/forever/node_modules/cliff/node_modules/winston/node_modules/request/tests/test-oauth.js` — `, oauth_token: "…[redacted 49 chars]"` (fingerprint b67188b03721; added in commit a7b556da2a25; removed from the working tree but recoverable by anyone with repository access)

Hardcoded credential assignment in git history

`security` · source: scanner (secrets) · effort: M · id `0b2613d12ff487ae`

Hardcoded credential assignment found in node_modules/forever/node_modules/cliff/node_modules/winston/node_modules/request/tests/test-oauth.js. The value is redacted here and identified by fingerprint.

Impact. Anyone who can read this code or its history holds a working credential. Rotation is required regardless of whether the file is still present.

Remediation. Rotate the credential now. Move it to a secret manager or environment variable. Purge it from git history (git filter-repo) before the repository moves anywhere.

Effort. M: rotate the credential, then rewrite history every clone must take (scanner rule secrets.credential_history)

Evidence.

- `node_modules/forever/node_modules/cliff/node_modules/winston/node_modules/request/tests/test-oauth.js` — `, consumer_secret: "…[redacted 43 chars]"` (fingerprint c70776c1ab86; added in commit a7b556da2a25; removed from the working tree but recoverable by anyone with repository access)

Hardcoded credential assignment in git history

`security` · source: scanner (secrets) · effort: M · id `b4638dcca84b078f`

Hardcoded credential assignment found in node_modules/forever/node_modules/cliff/node_modules/winston/node_modules/request/tests/test-oauth.js. The value is redacted here and identified by fingerprint.

Impact. Anyone who can read this code or its history holds a working credential. Rotation is required regardless of whether the file is still present.

Remediation. Rotate the credential now. Move it to a secret manager or environment variable. Purge it from git history (git filter-repo) before the repository moves anywhere.

Effort. M: rotate the credential, then rewrite history every clone must take (scanner rule secrets.credential_history)

Evidence.

- `node_modules/forever/node_modules/cliff/node_modules/winston/node_modules/request/tests/test-oauth.js` — `, token_secret: "…[redacted 41 chars]"` (fingerprint f6eca49d1a5a; added in commit a7b556da2a25; removed from the working tree but recoverable by anyone with repository access)

Hardcoded credential assignment in git history

`security` · source: scanner (secrets) · effort: M · id `c6facae95fb4e39a`

Hardcoded credential assignment found in node_modules/forever/node_modules/cliff/node_modules/winston/node_modules/request/tests/test-oauth.js. The value is redacted here and identified by fingerprint.

Impact. Anyone who can read this code or its history holds a working credential. Rotation is required regardless of whether the file is still present.

Remediation. Rotate the credential now. Move it to a secret manager or environment variable. Purge it from git history (git filter-repo) before the repository moves anywhere.

Effort. M: rotate the credential, then rewrite history every clone must take (scanner rule secrets.credential_history)

Evidence.

- `node_modules/forever/node_modules/cliff/node_modules/winston/node_modules/request/tests/test-oauth.js` — `, token_secret: "…[redacted 40 chars]"` (fingerprint 760e778aa414; added in commit a7b556da2a25; removed from the working tree but recoverable by anyone with repository access)

AWS access key ID in git history

`security` · source: scanner (secrets) · effort: M · id `87a94a8d62ec0bf6`

AWS access key ID found in node_modules/forever/node_modules/cliff/node_modules/winston/node_modules/request/tests/test-s3.js. The value is redacted here and identified by fingerprint.

Impact. Anyone who can read this code or its history holds a working credential. Rotation is required regardless of whether the file is still present.

Remediation. Rotate the credential now. Move it to a secret manager or environment variable. Purge it from git history (git filter-repo) before the repository moves anywhere.

Effort. M: rotate the credential, then rewrite history every clone must take (scanner rule secrets.credential_history)

Evidence.

- `node_modules/forever/node_modules/cliff/node_modules/winston/node_modules/request/tests/test-s3.js` — `{ key: 'AKIA…[redacted 20 chars]'` (fingerprint 4c114c2771d9; added in commit a7b556da2a25; removed from the working tree but recoverable by anyone with repository access)

Hardcoded credential assignment in git history

`security` · source: scanner (secrets) · effort: M · id `a6601bcd8c8741bd`

Hardcoded credential assignment found in node_modules/forever/node_modules/cliff/node_modules/winston/node_modules/request/tests/test-s3.js. The value is redacted here and identified by fingerprint.

Impact. Anyone who can read this code or its history holds a working credential. Rotation is required regardless of whether the file is still present.

Remediation. Rotate the credential now. Move it to a secret manager or environment variable. Purge it from git history (git filter-repo) before the repository moves anywhere.

Effort. M: rotate the credential, then rewrite history every clone must take (scanner rule secrets.credential_history)

Evidence.

- `node_modules/forever/node_modules/cliff/node_modules/winston/node_modules/request/tests/test-s3.js` — `, secret: '…[redacted 40 chars]'` (fingerprint 6f273c6c53d8; added in commit a7b556da2a25; removed from the working tree but recoverable by anyone with repository access)

Private key material in git history

`security` · source: scanner (secrets) · effort: M · id `33f4705eb2119d04`

Private key material found in node_modules/forever/node_modules/cliff/node_modules/winston/test/fixtures/keys/agent2-key.pem. The value is redacted here and identified by fingerprint.

Impact. Anyone who can read this code or its history holds a working credential. Rotation is required regardless of whether the file is still present.

Remediation. Rotate the credential now. Move it to a secret manager or environment variable. Purge it from git history (git filter-repo) before the repository moves anywhere.

Effort. M: rotate the credential, then rewrite history every clone must take (scanner rule secrets.credential_history)

Evidence.

- `node_modules/forever/node_modules/cliff/node_modules/winston/test/fixtures/keys/agent2-key.pem` — `…[redacted 31 chars]` (fingerprint 72d6cea4370e; added in commit a7b556da2a25; removed from the working tree but recoverable by anyone with repository access)

Hardcoded credential assignment in git history

`security` · source: scanner (secrets) · effort: M · id `faf846bea2f53656`

Hardcoded credential assignment found in node_modules/forever/node_modules/cliff/node_modules/winston/test/transports/webhook-test.js. The value is redacted here and identified by fingerprint.

Impact. Anyone who can read this code or its history holds a working credential. Rotation is required regardless of whether the file is still present.

Remediation. Rotate the credential now. Move it to a secret manager or environment variable. Purge it from git history (git filter-repo) before the repository moves anywhere.

Effort. M: rotate the credential, then rewrite history every clone must take (scanner rule secrets.credential_history)

Evidence.

- `node_modules/forever/node_modules/cliff/node_modules/winston/test/transports/webhook-test.js` — `"password": "…[redacted 9 chars]"` (fingerprint f1af8d890750; added in commit a7b556da2a25; removed from the working tree but recoverable by anyone with repository access)

Hardcoded credential assignment in git history

`security` · source: scanner (secrets) · effort: M · id `fceff1660cd5f827`

Hardcoded credential assignment found in node_modules/forever/node_modules/flatiron/node_modules/prompt/README.md. The value is redacted here and identified by fingerprint.

Impact. Anyone who can read this code or its history holds a working credential. Rotation is required regardless of whether the file is still present.

Remediation. Rotate the credential now. Move it to a secret manager or environment variable. Purge it from git history (git filter-repo) before the repository moves anywhere.

Effort. M: rotate the credential, then rewrite history every clone must take (scanner rule secrets.credential_history)

Evidence.

- `node_modules/forever/node_modules/flatiron/node_modules/prompt/README.md` — `password: '…[redacted 12 chars]',` (fingerprint 5e9dd8b43e30; added in commit a7b556da2a25; removed from the working tree but recoverable by anyone with repository access)

Private key material in git history

`security` · source: scanner (secrets) · effort: M · id `e9d26d9f9235fa58`

Private key material found in node_modules/forever/node_modules/nssocket/test/fixtures/ryans-key.pem. The value is redacted here and identified by fingerprint.

Impact. Anyone who can read this code or its history holds a working credential. Rotation is required regardless of whether the file is still present.

Remediation. Rotate the credential now. Move it to a secret manager or environment variable. Purge it from git history (git filter-repo) before the repository moves anywhere.

Effort. M: rotate the credential, then rewrite history every clone must take (scanner rule secrets.credential_history)

Evidence.

- `node_modules/forever/node_modules/nssocket/test/fixtures/ryans-key.pem` — `…[redacted 31 chars]` (fingerprint 0fbf77361b4c; added in commit a7b556da2a25; removed from the working tree but recoverable by anyone with repository access)

Private key material in git history

`security` · source: scanner (secrets) · effort: M · id `4469a99149e645df`

Private key material found in node_modules/grunt-contrib-watch/node_modules/tiny-lr/node_modules/faye-websocket/spec/server.key. The value is redacted here and identified by fingerprint.

Impact. Anyone who can read this code or its history holds a working credential. Rotation is required regardless of whether the file is still present.

Remediation. Rotate the credential now. Move it to a secret manager or environment variable. Purge it from git history (git filter-repo) before the repository moves anywhere.

Effort. M: rotate the credential, then rewrite history every clone must take (scanner rule secrets.credential_history)

Evidence.

- `node_modules/grunt-contrib-watch/node_modules/tiny-lr/node_modules/faye-websocket/spec/server.key` — `…[redacted 31 chars]` (fingerprint f579e02fd998; added in commit a7b556da2a25; removed from the working tree but recoverable by anyone with repository access)

Hardcoded credential assignment in git history

`security` · source: scanner (secrets) · effort: M · id `ba647a52c11a1dfd`

Hardcoded credential assignment found in node_modules/grunt-jsbeautifier/node_modules/js-beautify/js/lib/beautify-html.js. The value is redacted here and identified by fingerprint.

Impact. Anyone who can read this code or its history holds a working credential. Rotation is required regardless of whether the file is still present.

Remediation. Rotate the credential now. Move it to a secret manager or environment variable. Purge it from git history (git filter-repo) before the repository moves anywhere.

Effort. M: rotate the credential, then rewrite history every clone must take (scanner rule secrets.credential_history)

Evidence.

- `node_modules/grunt-jsbeautifier/node_modules/js-beautify/js/lib/beautify-html.js` — `single_token: '…[redacted 92 chars]'.split(','), //all the single tags for HTML` (fingerprint bb793c3f0822; added in commit a7b556da2a25; removed from the working tree but recoverable by anyone with repository access)

Database connection string with embedded password in git history

`security` · source: scanner (secrets) · effort: M · id `e89b87e0d5f017a6`

Database connection string with embedded password found in node_modules/mongodb/lib/mongodb/connection/url_parser.js. The value is redacted here and identified by fingerprint.

Impact. Anyone who can read this code or its history holds a working credential. Rotation is required regardless of whether the file is still present.

Remediation. Rotate the credential now. Move it to a secret manager or environment variable. Purge it from git history (git filter-repo) before the repository moves anywhere.

Effort. M: rotate the credential, then rewrite history every clone must take (scanner rule secrets.credential_history)

Evidence.

- `node_modules/mongodb/lib/mongodb/connection/url_parser.js` — `throw Error("URL must be in the format mongodb://user:…[redacted 4 chars]@host:port/dbname");` (fingerprint d74ff0ee8da3; added in commit a7b556da2a25; removed from the working tree but recoverable by anyone with repository access)

Known vulnerabilities in adm-zip 0.4.4

`dependency` · source: scanner (dependencies) · effort: S · id `1ad4f47ca5626665`

8 published advisories affect adm-zip 0.4.4 (npm), declared in package-lock.json: GHSA-3v6h-hqm4-2rg6: Arbitrary File Write in adm-zip; GHSA-7q85-xj36-vmfc: adm-zip: Uncontrolled memory allocation via the declared uncompressed size (DoS); GHSA-8238-w5pm-2374: adm-zip: Unhandled error event in async DEFLATE decompression crashes Node.js process (DoS); GHSA-c6fg-446q-cg94: adm-zip: getDataAsync() bypasses the maxOutputLength size guard enforced by the synchronous getData() path; GHSA-j5f4-cc29-5×44: adm-zip extraction preserves SUID/SGID bits from untrusted ZIPs → local privilege escalation; GHSA-p634-w6r4-rjp2: adm-zip: Duplicate ZIP entry names: getEntry() and extractAllTo() resolve to different content; GHSA-rcw4-f5rp-g42v: adm-

zip: Decompression-bomb protection (fix for CVE-2026-39244) can be bypassed by declaring uncompressed size as 0; GHSA-xcpc-8h2w-3j85: adm-zip: Crafted ZIP file triggers 4GB memory allocation.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade adm-zip to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-3v6h-hqm4-2rg6, GHSA-7q85-xj36-vmfc, GHSA-8238-w5pm-2374, GHSA-c6fg-446q-cg94, GHSA-j5f4-cc29-5×44, GHSA-p634-w6r4-rjp2, GHSA-rcw4-f5rp-g42v, GHSA-xcpc-8h2w-3j85)

Known vulnerabilities in ansi-regex 3.0.0

`dependency` · source: scanner (dependencies) · effort: S · id `5afab38d62475c33`

1 published advisory affects ansi-regex 3.0.0 (npm), declared in package-lock.json: GHSA-93q8-gq69-wqmw: Inefficient Regular Expression Complexity in chalk/ansi-regex.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade ansi-regex to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-93q8-gq69-wqmw)

Known vulnerabilities in async 2.6.1

`dependency` · source: scanner (dependencies) · effort: S · id `f7e2ce9e78e5db10`

1 published advisory affects async 2.6.1 (npm), declared in package-lock.json: GHSA-fwr7-v2mv-hh25: Prototype Pollution in async.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade async to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-fwr7-v2mv-hh25)

Known vulnerabilities in body-parser 1.18.3

`dependency` · source: scanner (dependencies) · effort: S · id `3869a80a7ff7d87a`

3 published advisories affect body-parser 1.18.3 (npm), declared in package-lock.json: GHSA-27r3-jxmh-p828: body-parser vulnerable to Denial of Service via trailing bytes after a compressed request body; GHSA-qwcr-r2fm-qrc7: body-parser vulnerable to denial of service when url encoding is enabled; GHSA-v422-hmwv-36×6: body-parser vulnerable to denial of service when invalid limit value silently disables size enforcement.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade body-parser to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-27r3-jxmh-p828, GHSA-qwcr-r2fm-qrc7, GHSA-v422-hmwv-36×6)

Known vulnerabilities in brace-expansion 1.1.11

`dependency` · source: scanner (dependencies) · effort: S · id `465c9e03c1f1a676`

8 published advisories affect brace-expansion 1.1.11 (npm), declared in package-lock.json: GHSA-3jxr-9vmj-r5cp: brace-expansion: DoS via exponential-time expansion of consecutive non-expanding {} groups; GHSA-6j4f-fj2g-mc7p: brace-expansion: DoS via uncontrolled recursion in parseCommaParts causing stack exhaustion; GHSA-f886-m6hf-6m8v: brace-expansion: Zero-step sequence causes process hang and memory exhaustion; GHSA-mh99-v99m-4gvg: brace-expansion: DoS via unbounded expansion length causing an out-of-memory process crash; GHSA-q2hr-2g5m-vwhr: brace-expansion: Quadratic-time expansion of the `{a},b}` rewrite causes CPU denial of service; GHSA-qhr7-859c-m2p7: brace-expansion: DoS via uncontrolled recursion on

nested brace groups causing stack exhaustion; GHSA-rgw5-rvv9-x895: brace-expansion: DoS via unbounded intermediate arrays, bypassing the CVE-2026-14257 mitigation; GHSA-v6h2-p8h4-qcjw: brace-expansion Regular Expression Denial of Service vulnerability.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade brace-expansion to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-3jxr-9vmj-r5cp, GHSA-6j4f-fj2g-mc7p, GHSA-f886-m6hf-6m8v, GHSA-mh99-v99m-4gvg, GHSA-q2hr-2g5m-vwhr, GHSA-qhr7-859c-m2p7, GHSA-rgw5-rvv9-x895, GHSA-v6h2-p8h4-qcjw)

Known vulnerabilities in brace-expansion 1.1.6

`dependency` · source: scanner (dependencies) · effort: S · id `c6be1eb3045a51db`

9 published advisories affect brace-expansion 1.1.6 (npm), declared in package-lock.json: GHSA-3jxr-9vmj-r5cp: brace-expansion: DoS via exponential-time expansion of consecutive non-expanding {} groups; GHSA-6j4f-fj2g-mc7p: brace-expansion: DoS via uncontrolled recursion in parseCommaParts causing stack exhaustion; GHSA-832h-xg76-4gv6: ReDoS in brace-expansion; GHSA-f886-m6hf-6m8v: brace-expansion: Zero-step sequence causes process hang and memory exhaustion; GHSA-mh99-v99m-4gvg: brace-expansion: DoS via unbounded expansion length causing an out-of-memory process crash; GHSA-q2hr-2g5m-vwhr: brace-expansion: Quadratic-time expansion of the `{a},b}` rewrite causes CPU denial of service; GHSA-qhr7-859c-m2p7: brace-expansion: DoS via uncontrolled recursion on nested brace groups causing stack exhaustion; GHSA-rgw5-rvv9-x895: brace-expansion: DoS via unbounded intermediate arrays, bypassing the CVE-2026-14257 mitigation; GHSA-v6h2-p8h4-qcjw: brace-expansion Regular Expression Denial of Service vulnerability.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade brace-expansion to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-3jxr-9vmj-r5cp, GHSA-6j4f-fj2g-mc7p, GHSA-832h-xg76-4gv6, GHSA-f886-m6hf-6m8v, GHSA-mh99-v99m-4gvg, GHSA-q2hr-2g5m-vwhr, GHSA-qhr7-859c-m2p7, GHSA-rgw5-rvv9-x895, GHSA-v6h2-p8h4-qcjw)

Known vulnerabilities in braces 1.8.5

`dependency` · source: scanner (dependencies) · effort: S · id `49c135ac5d138a4e`

1 published advisory affects braces 1.8.5 (npm), declared in package-lock.json: GHSA-grv7-fg5c-xmjg: Uncontrolled resource consumption in braces.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade braces to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-grv7-fg5c-xmjg)

Known vulnerabilities in braces 2.3.2

`dependency` · source: scanner (dependencies) · effort: S · id `8e5b2da52c1c0d44`

1 published advisory affects braces 2.3.2 (npm), declared in package-lock.json: GHSA-grv7-fg5c-xmjg: Uncontrolled resource consumption in braces.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade braces to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-grv7-fg5c-xmjg)

Known vulnerabilities in cross-spawn 4.0.0

`dependency` · source: scanner (dependencies) · effort: S · id `dfe9dadb5734b7ac`

1 published advisory affects cross-spawn 4.0.0 (npm), declared in package-lock.json: GHSA-3xgq-45jj-v275: Regular Expression Denial of Service (ReDoS) in cross-spawn.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade cross-spawn to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-3xgq-45jj-v275)

Known vulnerabilities in cross-spawn 4.0.2

`dependency` · source: scanner (dependencies) · effort: S · id `b5a12b72ff007682`

1 published advisory affects cross-spawn 4.0.2 (npm), declared in package-lock.json: GHSA-3xgq-45jj-v275: Regular Expression Denial of Service (ReDoS) in cross-spawn.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade cross-spawn to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-3xgq-45jj-v275)

Known vulnerabilities in cross-spawn 5.1.0

`dependency` · source: scanner (dependencies) · effort: S · id `7ed6be60ee7f051f`

1 published advisory affects cross-spawn 5.1.0 (npm), declared in package-lock.json: GHSA-3xgq-45jj-v275: Regular Expression Denial of Service (ReDoS) in cross-spawn.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade cross-spawn to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-3xgq-45jj-v275)

Known vulnerabilities in cross-spawn 6.0.5

`dependency` · source: scanner (dependencies) · effort: S · id `9d3be9d4d7836414`

1 published advisory affects cross-spawn 6.0.5 (npm), declared in package-lock.json: GHSA-3xgq-45jj-v275: Regular Expression Denial of Service (ReDoS) in cross-spawn.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade cross-spawn to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-3xgq-45jj-v275)

Known vulnerabilities in cross-spawn 7.0.3

`dependency` · source: scanner (dependencies) · effort: S · id `961689d517470666`

1 published advisory affects cross-spawn 7.0.3 (npm), declared in package-lock.json: GHSA-3xgq-45jj-v275: Regular Expression Denial of Service (ReDoS) in cross-spawn.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade cross-spawn to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-3xgq-45jj-v275)

Known vulnerabilities in debug 2.2.0

`dependency` · source: scanner (dependencies) · effort: S · id `c49afa4d0d2650d9`

2 published advisories affect debug 2.2.0 (npm), declared in package-lock.json: GHSA-9vvw-cc9w-f27h: debug Inefficient Regular Expression Complexity vulnerability; GHSA-gxpj-cx7g-858c: Regular Expression Denial of Service in debug.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade debug to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-9vvw-cc9w-f27h, GHSA-gxpj-cx7g-858c)

Known vulnerabilities in decode-uri-component 0.2.0

`dependency` · source: scanner (dependencies) · effort: S · id `9713a45504ae6c70`

3 published advisories affect decode-uri-component 0.2.0 (npm), declared in package-lock.json: GHSA-qr28-fpjm-wq7f: decode-uri-component vulnerable to denial of service via quadratic replacement of percent-encoded runs; GHSA-vcc3-ghjq-m6fr: decode-uri-component: Denial of service via exponential decoding of malformed percent-encoded input; GHSA-w573-4hg7-7wgq: decode-uri-component vulnerable to Denial of Service (DoS).

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade decode-uri-component to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-qr28-fpjm-wq7f, GHSA-vcc3-ghjq-m6fr, GHSA-w573-4hg7-7wgq)

Known vulnerabilities in diff 1.4.0

`dependency` · source: scanner (dependencies) · effort: S · id `0a1c783c82f3a702`

2 published advisories affect diff 1.4.0 (npm), declared in package-lock.json: GHSA-73rr-hh4g-fpgx: jsdiff has a Denial of Service vulnerability in parsePatch and applyPatch; GHSA-h6ch-v84p-w6p9: Regular Expression Denial of Service (ReDoS).

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade diff to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-73rr-hh4g-fpgx, GHSA-h6ch-v84p-w6p9)

Known vulnerabilities in dot-prop 4.2.0

`dependency` · source: scanner (dependencies) · effort: S · id `df2746eb9cd6e41b`

1 published advisory affects dot-prop 4.2.0 (npm), declared in package-lock.json: GHSA-ff7x-qrg7-qggm: dot-prop Prototype Pollution vulnerability.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade dot-prop to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-ff7x-qrg7-qggm)

Known vulnerabilities in extract-zip 1.6.7

`dependency` · source: scanner (dependencies) · effort: S · id `d4029d5c82e908db`

2 published advisories affect extract-zip 1.6.7 (npm), declared in package-lock.json: GHSA-7pqw-9j4j-h8q3: extract-zip allows arbitrary file writes through symlink archive entries; GHSA-jmr9-qjv8-65gv: extract-zip unvalidated symlink path traversal.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade extract-zip to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-7pqw-9j4j-h8q3, GHSA-jmr9-qjv8-65gv)

Known vulnerabilities in fstream 1.0.10

`dependency` · source: scanner (dependencies) · effort: S · id `3a6737956ac119e2`

1 published advisory affects fstream 1.0.10 (npm), declared in package-lock.json: GHSA-xf7w-r453-m56c: Arbitrary File Overwrite in fstream.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade fstream to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-xf7w-r453-m56c)

Known vulnerabilities in grunt 1.0.3

`dependency` · source: scanner (dependencies) · effort: S · id `6ed4c0da48cf72cc`

3 published advisories affect grunt 1.0.3 (npm), declared in package-lock.json: GHSA-j383-35pm-c5h4: Path Traversal in Grunt; GHSA-m5pj-vjjf-4m3h: Arbitrary Code Execution in grunt; GHSA-rm36-94g8-835r: Race Condition in Grunt.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade grunt to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-j383-35pm-c5h4, GHSA-m5pj-vjjf-4m3h, GHSA-rm36-94g8-835r)

Known vulnerabilities in hawk 1.0.0

`dependency` · source: scanner (dependencies) · effort: S · id `4771448224a2aa1a`

2 published advisories affect hawk 1.0.0 (npm), declared in package-lock.json: GHSA-44pw-h2cw-w3vq: Uncontrolled Resource Consumption in Hawk; GHSA-jcpv-g9rr-qxrc: Regular Expression Denial of Service in hawk.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade hawk to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-44pw-h2cw-w3vq, GHSA-jcpv-g9rr-qxrc)

Known vulnerabilities in hawk 3.1.3

`dependency` · source: scanner (dependencies) · effort: S · id `d3ac3c16e84373b5`

1 published advisory affects hawk 3.1.3 (npm), declared in package-lock.json: GHSA-44pw-h2cw-w3vq: Uncontrolled Resource Consumption in Hawk.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade hawk to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-44pw-h2cw-w3vq)

Known vulnerabilities in hoek 0.9.1

`dependency` · source: scanner (dependencies) · effort: S · id `02428b9f37bd34a7`

2 published advisories affect hoek 0.9.1 (npm), declared in package-lock.json: GHSA-c429-5p7v-vgjp: hoek subject to prototype pollution via the clone function.; GHSA-jp4x-w63m-7wgm: Prototype Pollution in hoek.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade hoek to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-c429-5p7v-vgjp, GHSA-jp4x-w63m-7wgm)

Known vulnerabilities in hoek 2.16.3

`dependency` · source: scanner (dependencies) · effort: S · id `fcf93e1f414ea1db`

2 published advisories affect hoek 2.16.3 (npm), declared in package-lock.json: GHSA-c429-5p7v-vgjp: hoek subject to prototype pollution via the clone function.; GHSA-jp4x-w63m-7wgm: Prototype Pollution in hoek.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade hoek to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-c429-5p7v-vgjp, GHSA-jp4x-w63m-7wgm)

Known vulnerabilities in i 0.3.6

`dependency` · source: scanner (dependencies) · effort: S · id `881be7af48c5ef6c`

1 published advisory affects i 0.3.6 (npm), declared in package-lock.json: GHSA-x55w-vjjp-222r: inflect vulnerable to Inefficient Regular Expression Complexity.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade i to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-x55w-vjjp-222r)

Known vulnerabilities in ini 1.3.4

`dependency` · source: scanner (dependencies) · effort: S · id `1e2d06f7979427c8`

1 published advisory affects ini 1.3.4 (npm), declared in package-lock.json: GHSA-qqgx-2p2h-9c37: ini before 1.3.6 vulnerable to Prototype Pollution via ini.parse.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade ini to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-qqgx-2p2h-9c37)

Known vulnerabilities in ini 1.3.5

`dependency` · source: scanner (dependencies) · effort: S · id `179cdd59e972a231`

1 published advisory affects ini 1.3.5 (npm), declared in package-lock.json: GHSA-qqgx-2p2h-9c37: ini before 1.3.6 vulnerable to Prototype Pollution via ini.parse.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade ini to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-qqgx-2p2h-9c37)

Known vulnerabilities in js-yaml 3.5.5

`dependency` · source: scanner (dependencies) · effort: S · id `584f0296510880a2`

7 published advisories affect js-yaml 3.5.5 (npm), declared in package-lock.json: GHSA-2883-xcg3-v3hh: js-yaml: maxTotalMergeKeys does not limit CPU use for empty merge sources; GHSA-2pr6-76vf-7546: Denial of Service in js-yaml; GHSA-52cp-r559-cp3m: js-yaml: YAML merge-key chains can force quadratic CPU consumption; GHSA-5p4m-2wfm-xmqj: JS-YAML: Quadratic CPU consumption in !!omap resolution (3.x and 4.x) — CVE-2026-59870 fix not backported; GHSA-8j8c-7jfh-h6hx: Code Injection in js-yaml; GHSA-h67p-54hq-rp68: JS-YAML: Quadratic-complexity DoS in merge key handling via repeated aliases; GHSA-mh29-5h37-fv8m: js-yaml has prototype pollution in merge (<<).

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade js-yaml to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-2883-xcg3-v3hh, GHSA-2pr6-76vf-7546, GHSA-52cp-r559-cp3m, GHSA-5p4m-2wfm-xmqj, GHSA-8j8c-7jfh-h6hx, GHSA-h67p-54hq-rp68, GHSA-mh29-5h37-fv8m)

Known vulnerabilities in js-yaml 3.6.1

`dependency` · source: scanner (dependencies) · effort: S · id `05d1c14ccdb8c7c5`

7 published advisories affect js-yaml 3.6.1 (npm), declared in package-lock.json: GHSA-2883-xcg3-v3hh: js-yaml: maxTotalMergeKeys does not limit CPU use for empty merge sources; GHSA-2pr6-76vf-7546: Denial of Service in js-yaml; GHSA-52cp-r559-cp3m: js-yaml: YAML merge-key chains can force quadratic CPU consumption; GHSA-5p4m-2wfm-xmqj: JS-YAML: Quadratic CPU consumption in !!omap resolution (3.x and 4.x) — CVE-2026-59870 fix not backported; GHSA-8j8c-7jfh-h6hx: Code Injection in js-yaml; GHSA-h67p-54hq-rp68: JS-YAML: Quadratic-complexity DoS in merge key handling via repeated aliases; GHSA-mh29-5h37-fv8m: js-yaml has prototype pollution in merge (<<).

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade js-yaml to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-2883-xcg3-v3hh, GHSA-2pr6-76vf-7546, GHSA-52cp-r559-cp3m, GHSA-5p4m-2wfm-xmqj, GHSA-8j8c-7jfh-h6hx, GHSA-h67p-54hq-rp68, GHSA-mh29-5h37-fv8m)

Known vulnerabilities in kind-of 6.0.2

`dependency` · source: scanner (dependencies) · effort: S · id `e2d76d12e6b396aa`

1 published advisory affects kind-of 6.0.2 (npm), declared in package-lock.json: GHSA-6c8f-qphg-qjgp: Validation Bypass in kind-of.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade kind-of to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-6c8f-qphg-qjgp)

Known vulnerabilities in lodash 4.17.20

`dependency` · source: scanner (dependencies) · effort: S · id `363d292685451735`

4 published advisories affect lodash 4.17.20 (npm), declared in package-lock.json: GHSA-29mw-wpgm-hmr9: Regular Expression Denial of Service (ReDoS) in lodash; GHSA-35jh-r3h4-6jhm: Command Injection in lodash; GHSA-r5fr-rjxr-66jc: lodash vulnerable to Code Injection via `_.template` imports key names; GHSA-xxjr-mmjv-4gpg: Lodash has Prototype Pollution Vulnerability in `_.unset`, `_.omit`, and `_.pullAt` functions.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade lodash to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-29mw-wpgm-hmr9, GHSA-35jh-r3h4-6jhm, GHSA-r5fr-rjxr-66jc, GHSA-xxjr-mmjv-4gpg)

Known vulnerabilities in lodash 4.17.21

`dependency` · source: scanner (dependencies) · effort: S · id `acee990e95b57170`

2 published advisories affect lodash 4.17.21 (npm), declared in package-lock.json: GHSA-r5fr-rjxr-66jc: lodash vulnerable to Code Injection via `_.template` imports key names; GHSA-xxjr-mmjv-4gpg: Lodash has Prototype Pollution Vulnerability in `_.unset`, `_.omit`, and `_.pullAt` functions.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade lodash to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-r5fr-rjxr-66jc, GHSA-xxjr-mmjv-4gpg)

Known vulnerabilities in marked 0.3.5

`dependency` · source: scanner (dependencies) · effort: S · id `38861c70750604f1`

6 published advisories affect marked 0.3.5 (npm), declared in package-lock.json: GHSA-5v2h-r2cx-5xgj: Inefficient Regular Expression Complexity in marked; GHSA-7px7-7xjx-hxm8: Marked vulnerable to XSS from data URIs; GHSA-p9wx-2529-fp83: Marked allows Regular Expression Denial of Service (ReDoS) attacks; GHSA-rrrm-qjm4-v8hf: Inefficient Regular Expression Complexity in marked; GHSA-vfvf-mqq8-rwqc: Sanitization bypass using HTML Entities in marked; GHSA-x5pg-88wf-qq4p: Regular Expression Denial of Service in marked.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade marked to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-5v2h-r2cx-5xgj, GHSA-7px7-7xjx-hxm8, GHSA-p9wx-2529-fp83, GHSA-rrrm-qjm4-v8hf, GHSA-vfvf-mqq8-rwqc, GHSA-x5pg-88wf-qq4p)

Known vulnerabilities in mime 1.2.11

`dependency` · source: scanner (dependencies) · effort: S · id `f02d9e65d0484b0f`

1 published advisory affects mime 1.2.11 (npm), declared in package-lock.json: GHSA-wrvr-8mpx-r7pp: mime Regular Expression Denial of Service when MIME lookup performed on untrusted user input.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade mime to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-wrvr-8mpx-r7pp)

Known vulnerabilities in minimatch 0.3.0

`dependency` · source: scanner (dependencies) · effort: S · id `5f28de816709197c`

5 published advisories affect minimatch 0.3.0 (npm), declared in package-lock.json: GHSA-23c5-xmqv-rm74: minimatch ReDoS: nested *() extglobs generate catastrophically backtracking regular expressions; GHSA-3ppc-4f35-3m26: minimatch has a ReDoS via repeated wildcards with non-matching literal in pattern; GHSA-7r86-cg39-jmmj: minimatch has ReDoS: matchOne() combinatorial backtracking via multiple non-adjacent GLOBSTAR segments; GHSA-f8q6-p94x-37v3: minimatch ReDoS vulnerability; GHSA-hxm2-r34f-qmc5: Regular Expression Denial of Service in minimatch.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade minimatch to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-23c5-xmqv-rm74, GHSA-3ppc-4f35-3m26, GHSA-7r86-cg39-jmmj, GHSA-f8q6-p94x-37v3, GHSA-hxm2-r34f-qmc5)

Known vulnerabilities in minimatch 3.0.2

`dependency` · source: scanner (dependencies) · effort: S · id `c9acac164262a463`

4 published advisories affect minimatch 3.0.2 (npm), declared in package-lock.json: GHSA-23c5-xmqv-rm74: minimatch ReDoS: nested *() extglobs generate catastrophically backtracking regular expressions; GHSA-3ppc-4f35-3m26: minimatch has a ReDoS via repeated wildcards with non-matching literal in pattern; GHSA-7r86-cg39-jmmj: minimatch has ReDoS: matchOne() combinatorial backtracking via multiple non-adjacent GLOBSTAR segments; GHSA-f8q6-p94x-37v3: minimatch ReDoS vulnerability.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade minimatch to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-23c5-xmqv-rm74, GHSA-3ppc-4f35-3m26, GHSA-7r86-cg39-jmmj, GHSA-f8q6-p94x-37v3)

Known vulnerabilities in minimatch 3.0.3

`dependency` · source: scanner (dependencies) · effort: S · id `59d4e4e1f5e7fade`

4 published advisories affect minimatch 3.0.3 (npm), declared in package-lock.json: GHSA-23c5-xmqv-rm74: minimatch ReDoS: nested *() extglobs generate catastrophically backtracking regular expressions; GHSA-3ppc-4f35-3m26: minimatch has a ReDoS via repeated wildcards with non-matching literal in pattern; GHSA-7r86-cg39-jmmj: minimatch has ReDoS: matchOne() combinatorial backtracking via multiple non-adjacent GLOBSTAR segments; GHSA-f8q6-p94x-37v3: minimatch ReDoS vulnerability.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade minimatch to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-23c5-xmqv-rm74, GHSA-3ppc-4f35-3m26, GHSA-7r86-cg39-jmmj, GHSA-f8q6-p94x-37v3)

Known vulnerabilities in minimatch 3.0.4

`dependency` · source: scanner (dependencies) · effort: S · id `8ca94da4bfe47848`

4 published advisories affect minimatch 3.0.4 (npm), declared in package-lock.json: GHSA-23c5-xmqv-rm74: minimatch ReDoS: nested *() extglobs generate catastrophically backtracking regular expressions; GHSA-3ppc-4f35-3m26: minimatch has a ReDoS via repeated wildcards with non-matching literal in pattern; GHSA-7r86-cg39-jmmj: minimatch has ReDoS: matchOne() combinatorial backtracking via multiple non-adjacent GLOBSTAR segments; GHSA-f8q6-p94x-37v3: minimatch ReDoS vulnerability.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade minimatch to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-23c5-xmqv-rm74, GHSA-3ppc-4f35-3m26, GHSA-7r86-cg39-jmmj, GHSA-f8q6-p94x-37v3)

Known vulnerabilities in moment 2.24.0

`dependency` · source: scanner (dependencies) · effort: S · id `88fa707b3df2196e`

2 published advisories affect moment 2.24.0 (npm), declared in package-lock.json: GHSA-8hfj-j24r-96c4: Path Traversal: 'dir/../../filename' in moment.locale; GHSA-wc69-rhjr-hc9g: Moment.js vulnerable to Inefficient Regular Expression Complexity.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade moment to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-8hfj-j24r-96c4, GHSA-wc69-rhjr-hc9g)

Known vulnerabilities in mongodb 2.2.36

`dependency` · source: scanner (dependencies) · effort: S · id `2758e0efeefd409e`

1 published advisory affects mongodb 2.2.36 (npm), declared in package-lock.json: GHSA-mh5c-679w-hh4r: Denial of Service in mongodb.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade mongodb to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-mh5c-679w-hh4r)

Known vulnerabilities in nconf 0.10.0

`dependency` · source: scanner (dependencies) · effort: S · id `cfeec70f02dc79cc`

1 published advisory affects nconf 0.10.0 (npm), declared in package-lock.json: GHSA-6xwr-q98w-rvg7: Prototype Pollution in nconf.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade nconf to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-6xwr-q98w-rvg7)

Known vulnerabilities in nconf 0.6.9

`dependency` · source: scanner (dependencies) · effort: S · id `61ca459443c1d16d`

1 published advisory affects nconf 0.6.9 (npm), declared in package-lock.json: GHSA-6xwr-q98w-rvg7: Prototype Pollution in nconf.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade nconf to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-6xwr-q98w-rvg7)

Known vulnerabilities in npm 3.10.10

`dependency` · source: scanner (dependencies) · effort: S · id `cbfe8a10bbddcf09`

5 published advisories affect npm 3.10.10 (npm), declared in package-lock.json: GHSA-4328-8hgf-7wjr: npm Vulnerable to Global node_modules Binary Overwrite; GHSA-93f3-23rq-pjfp: npm CLI exposing sensitive information through logs; GHSA-m6cx-g6qm-p2cx: Arbitrary File Write in npm; GHSA-ph34-pc88-72gc: Incorrect Permission Assignment for Critical Resource in NPM; GHSA-x8qc-rrcw-4r46: npm symlink reference outside of node_modules.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade npm to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-4328-8hgf-7wjr, GHSA-93f3-23rq-pjfp, GHSA-m6cx-g6qm-p2cx, GHSA-ph34-pc88-72gc, GHSA-x8qc-rrcw-4r46)

Known vulnerabilities in npm-user-validate 0.1.5

`dependency` · source: scanner (dependencies) · effort: S · id `082453e387c21e06`

1 published advisory affects npm-user-validate 0.1.5 (npm), declared in package-lock.json: GHSA-pw54-mh39-w3hc: Regular expression denial of service in npm-user-validate.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade npm-user-validate to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-pw54-mh39-w3hc)

Known vulnerabilities in path-to-regexp 0.1.7

`dependency` · source: scanner (dependencies) · effort: S · id `38140ebc257b38ca`

2 published advisories affect path-to-regexp 0.1.7 (npm), declared in package-lock.json: GHSA-37ch-88jc-xwx2: path-to-regexp vulnerable to Regular Expression Denial of Service via multiple route parameters; GHSA-rhx6-c78j-4q9w: path-to-regexp contains a ReDoS.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade path-to-regexp to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-37ch-88jc-xwx2, GHSA-rhx6-c78j-4q9w)

Known vulnerabilities in qs 0.6.6

`dependency` · source: scanner (dependencies) · effort: S · id `dc09b16210953d4a`

5 published advisories affect qs 0.6.6 (npm), declared in package-lock.json: GHSA-6rw7-vpxm-498p: qs's arrayLimit bypass in its bracket notation allows DoS via memory exhaustion; GHSA-f9cm-p3w6-xvr3: Denial-of-Service Extended Event Loop Blocking in qs; GHSA-gqgv-6jq5-jjj9: Prototype Pollution Protection Bypass in qs; GHSA-hrpp-h998-j3pp: qs vulnerable to Prototype Pollution; GHSA-jjv7-qpx3-h62q: Denial-of-Service Memory Exhaustion in qs.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade qs to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-6rw7-vpxm-498p, GHSA-f9cm-p3w6-xvr3, GHSA-gqgv-6jq5-jjj9, GHSA-hrpp-h998-j3pp, GHSA-jjv7-qpx3-h62q)

Known vulnerabilities in qs 5.2.1

`dependency` · source: scanner (dependencies) · effort: S · id `36322ef20aacef6e`

4 published advisories affect qs 5.2.1 (npm), declared in package-lock.json: GHSA-4mjr-xmp4-gh2g: qs: Denial of Service via Attacker Controlled isBuffer; GHSA-6rw7-vpxm-498p: qs's arrayLimit bypass in its bracket notation allows DoS via memory exhaustion; GHSA-gqgv-6jq5-jjj9: Prototype Pollution Protection Bypass in qs; GHSA-hrpp-h998-j3pp: qs vulnerable to Prototype Pollution.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade qs to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-4mjr-xmp4-gh2g, GHSA-6rw7-vpxm-498p, GHSA-gqgv-6jq5-jjj9, GHSA-hrpp-h998-j3pp)

Known vulnerabilities in qs 6.2.1

`dependency` · source: scanner (dependencies) · effort: S · id `e29852a7d99b3a70`

4 published advisories affect qs 6.2.1 (npm), declared in package-lock.json: GHSA-4mjr-xmp4-gh2g: qs: Denial of Service via Attacker Controlled isBuffer; GHSA-6rw7-vpxm-498p: qs's arrayLimit bypass in its bracket notation allows DoS via memory exhaustion; GHSA-gqgv-6jq5-jjj9: Prototype Pollution Protection Bypass in qs; GHSA-hrpp-h998-j3pp: qs vulnerable to Prototype Pollution.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade qs to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-4mjr-xmp4-gh2g, GHSA-6rw7-vpxm-498p, GHSA-gqgv-6jq5-jjj9, GHSA-hrpp-h998-j3pp)

Known vulnerabilities in qs 6.3.2

`dependency` · source: scanner (dependencies) · effort: S · id `6e228e015f8643ea`

3 published advisories affect qs 6.3.2 (npm), declared in package-lock.json: GHSA-4mjr-xmp4-gh2g: qs: Denial of Service via Attacker Controlled isBuffer; GHSA-6rw7-vpxm-498p: qs's arrayLimit bypass in its bracket notation allows DoS via memory exhaustion; GHSA-hrpp-h998-j3pp: qs vulnerable to Prototype Pollution.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade qs to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-4mjr-xmp4-gh2g, GHSA-6rw7-vpxm-498p, GHSA-hrpp-h998-j3pp)

Known vulnerabilities in qs 6.5.2

`dependency` · source: scanner (dependencies) · effort: S · id `5b43efe875b1c346`

3 published advisories affect qs 6.5.2 (npm), declared in package-lock.json: GHSA-4mjr-xmp4-gh2g: qs: Denial of Service via Attacker Controlled isBuffer; GHSA-6rw7-vpxm-498p: qs's arrayLimit bypass in its bracket notation allows DoS via memory exhaustion; GHSA-hrpp-h998-j3pp: qs vulnerable to Prototype Pollution.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade qs to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-4mjr-xmp4-gh2g, GHSA-6rw7-vpxm-498p, GHSA-hrpp-h998-j3pp)

Known vulnerabilities in semver 5.3.0

`dependency` · source: scanner (dependencies) · effort: S · id `eae36d29179e999b`

1 published advisory affects semver 5.3.0 (npm), declared in package-lock.json: GHSA-c2qf-rxjj-qqgw: semver vulnerable to Regular Expression Denial of Service.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade semver to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-c2qf-rxjj-qqgw)

Known vulnerabilities in semver 5.6.0

`dependency` · source: scanner (dependencies) · effort: S · id `9ba832b07428d43e`

1 published advisory affects semver 5.6.0 (npm), declared in package-lock.json: GHSA-c2qf-rxjj-qqgw: semver vulnerable to Regular Expression Denial of Service.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade semver to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-c2qf-rxjj-qqgw)

Known vulnerabilities in semver 5.7.0

`dependency` · source: scanner (dependencies) · effort: S · id `06f5450267b48273`

1 published advisory affects semver 5.7.0 (npm), declared in package-lock.json: GHSA-c2qf-rxjj-qqgw: semver vulnerable to Regular Expression Denial of Service.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade semver to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-c2qf-rxjj-qqgw)

Known vulnerabilities in shelljs 0.3.0

`dependency` · source: scanner (dependencies) · effort: S · id `c54221081567f493`

2 published advisories affect shelljs 0.3.0 (npm), declared in package-lock.json: GHSA-4rq4-32rv-6wp6: Improper Privilege Management in shelljs; GHSA-64g7-mvw6-v9qj: Improper Privilege Management in shelljs.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade shelljs to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-4rq4-32rv-6wp6, GHSA-64g7-mvw6-v9qj)

Known vulnerabilities in sshpk 1.10.1

`dependency` · source: scanner (dependencies) · effort: S · id `cbbde1db3b7b8bcb`

1 published advisory affects sshpk 1.10.1 (npm), declared in package-lock.json: GHSA-2m39-62fm-q8r3: Regular Expression Denial of Service in sshpk.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade sshpk to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-2m39-62fm-q8r3)

Known vulnerabilities in swig 1.4.2

`dependency` · source: scanner (dependencies) · effort: S · id `e7342b1ff1ade27c`

1 published advisory affects swig 1.4.2 (npm), declared in package-lock.json: GHSA-2rq5-699j-x7p6: Arbitrary local file read vulnerability during template rendering .

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade swig to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-2rq5-699j-x7p6)

Known vulnerabilities in tmp 0.0.24

`dependency` · source: scanner (dependencies) · effort: S · id `a6300799c416e2bb`

2 published advisories affect tmp 0.0.24 (npm), declared in package-lock.json: GHSA-52f5-9888-hmc6: tmp allows arbitrary temporary file / directory write via symbolic link `dir` parameter; GHSA-ph9p-34f9-6g65: tmp has Path Traversal via unsanitized prefix/postfix that enables directory escape.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade tmp to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-52f5-9888-hmc6, GHSA-ph9p-34f9-6g65)

Known vulnerabilities in tmp 0.1.0

`dependency` · source: scanner (dependencies) · effort: S · id `4e559af49391b80c`

2 published advisories affect tmp 0.1.0 (npm), declared in package-lock.json: GHSA-52f5-9888-hmc6: tmp allows arbitrary temporary file / directory write via symbolic link `dir` parameter; GHSA-ph9p-34f9-6g65: tmp has Path Traversal via unsanitized prefix/postfix that enables directory escape.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade tmp to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-52f5-9888-hmc6, GHSA-ph9p-34f9-6g65)

Known vulnerabilities in tough-cookie 2.2.2

`dependency` · source: scanner (dependencies) · effort: S · id `dea7815dc79483d9`

3 published advisories affect tough-cookie 2.2.2 (npm), declared in package-lock.json: GHSA-72xf-g2v4-qvf3: tough-cookie Prototype Pollution vulnerability; GHSA-g7q5-pjjr-gqvp: Regular Expression Denial of Service in tough-cookie; GHSA-qhv9-728r-6jqg: ReDoS via long string of semicolons in tough-cookie.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade tough-cookie to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-72xf-g2v4-qvf3, GHSA-g7q5-pjjr-gqvp, GHSA-qhv9-728r-6jqg)

Known vulnerabilities in tough-cookie 2.3.1

`dependency` · source: scanner (dependencies) · effort: S · id `ae1a749c3c85562d`

2 published advisories affect tough-cookie 2.3.1 (npm), declared in package-lock.json: GHSA-72xf-g2v4-qvf3: tough-cookie Prototype Pollution vulnerability; GHSA-g7q5-pjjr-gqvp: Regular Expression Denial of Service in tough-cookie.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade tough-cookie to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-72xf-g2v4-qvf3, GHSA-g7q5-pjjr-gqvp)

Known vulnerabilities in trim-newlines 1.0.0

`dependency` · source: scanner (dependencies) · effort: S · id `20ac97e64349a405`

1 published advisory affects trim-newlines 1.0.0 (npm), declared in package-lock.json: GHSA-7p7h-4mm5-852v: Uncontrolled Resource Consumption in trim-newlines.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade trim-newlines to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-7p7h-4mm5-852v)

Known vulnerabilities in uglify-js 2.4.24

`dependency` · source: scanner (dependencies) · effort: S · id `0a9482ef323371f4`

1 published advisory affects uglify-js 2.4.24 (npm), declared in package-lock.json: GHSA-c9f4-xj24-8jqx: Regular Expression Denial of Service in uglify-js.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade uglify-js to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-c9f4-xj24-8jqx)

Known vulnerabilities in uuid 3.3.2

`dependency` · source: scanner (dependencies) · effort: S · id `bfde9ae5afd31364`

1 published advisory affects uuid 3.3.2 (npm), declared in package-lock.json: GHSA-w5hq-g745-h8pq: uuid: Missing buffer bounds check in v3/v5/v6 when buf is provided.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade uuid to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-w5hq-g745-h8pq)

Known vulnerabilities in websocket-extensions 0.1.3

`dependency` · source: scanner (dependencies) · effort: S · id `20a0281a8c1d5608`

1 published advisory affects websocket-extensions 0.1.3 (npm), declared in package-lock.json: GHSA-g78m-2chm-r7qv: Regular Expression Denial of Service in websocket-extensions (NPM package).

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade websocket-extensions to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-g78m-2chm-r7qv)

Known vulnerabilities in ws 1.1.5

`dependency` · source: scanner (dependencies) · effort: S · id `5399bd80853367b8`

1 published advisory affects ws 1.1.5 (npm), declared in package-lock.json: GHSA-96hv-2xvq-fx4p: ws: Memory exhaustion DoS from tiny fragments and data chunks.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade ws to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-96hv-2xvq-fx4p)

Known vulnerabilities in y18n 3.2.1

`dependency` · source: scanner (dependencies) · effort: S · id `4a76ba2d2b651c3a`

1 published advisory affects y18n 3.2.1 (npm), declared in package-lock.json: GHSA-c4w7-xm78-47vh: Prototype Pollution in y18n.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade y18n to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-c4w7-xm78-47vh)

Medium (37)

Bulk commits

`process` · source: scanner (generated_bulk) · effort: L · id `51577234fe744da5`

7 commit(s) each changed more than 2,000 lines (677,783 lines, 51% of all changed lines).

Impact. Changes this large are rarely reviewed line by line; they are typical of generated code pasted in wholesale, so defects and copied secrets slip through.

Remediation. Review the largest of these commits for code nobody owns, and require smaller, reviewed changes from now on.

Effort. L: review the largest unreviewed commits (scanner rule generated_bulk.bulk_commits)

Evidence.

- `.` (a7b556da2a25 2013-12-02 Chetan Karande: +625,625 -1 in 4313 file(s): Included node_modules for faster and consistent deployemnts)
- `.` (5848aad1d8b4 2023-03-06 Liran Tal: +15,684 -924 in 2 file(s): fix: revert marked changes back to make sure we use the vulnerable version)
- `.` (aad96e69ce76 2019-03-03 ckarande: +11,290 -0 in 1 file(s): Update package versions)
- `.` (a58571ada601 2013-11-17 Chetan Karande: +9,837 -0 in 47 file(s): closes #1, closes #3, closes #4, closes #5, closes #6)
- `.` (60f02d28b384 2019-08-07 Josep: +3,384 -3,410 in 3 file(s): Add nodemon as npm script)
- `.` (7593798f995e 2020-04-02 fabre-pierre-jean: +2,744 -2,064 in 3 file(s): add forever node_modules)
- `.` (199e6b58e6a3 2014-03-11 Chetan Karande: +2,283 -537 in 57 file(s): Update for release)

Dependency or build directories in the source

`maintainability` · source: scanner (vendored_bulk) · effort: M · id `6b9252b3385d5a78`

1 directory of third-party or build output (15 files, 0.8 MB) are part of the source: app/assets/vendor.

Impact. Third-party code is versioned alongside the tool's own: it bloats every clone, hides local edits to dependencies, and never receives security updates.

Remediation. Remove these directories from the source, list them in .gitignore, and restore them from the package manager's manifest and lockfile at build time.

Effort. M: restore dependencies from the manifest at build time (scanner rule vendored_bulk.vendored_directories)

Evidence.

- `app/assets/vendor` (15 files, 0.8 MB)

Route handlers with no authentication check nearby

`security` · source: scanner (client_exposure) · effort: L · id `8b4a401cca718575`

15 route handler(s) in 2 file(s) have no authentication identifier (auth, session, jwt, current user, guard) near them. This is a heuristic for review: middleware or a wrapper elsewhere may protect them. Model extraction, when configured, is asked to confirm each one.

Impact. An unprotected handler that reads or changes data exposes it to anyone who can reach the server.

Remediation. Confirm each handler is protected; add authentication middleware or an explicit check where it is not.

Effort. L: confirm and add authentication across the handlers (scanner rule client_exposure.unauthenticated_routes)

Evidence.

- `app/routes/index.js:47` — `app.get("/profile", isLoggedIn, profileHandler.displayProfile);` (GET /profile)
- `app/routes/index.js:48` — `app.post("/profile", isLoggedIn, profileHandler.handleProfileUpdate);` (POST /profile)
- `app/routes/index.js:51` — `app.get("/contributions", isLoggedIn, contributionsHandler.displayContributions);` (GET /contributions)
- `app/routes/index.js:52` — `app.post("/contributions", isLoggedIn, contributionsHandler.handleContributionsUpdate);` (POST /contributions)
- `app/routes/index.js:55` — `app.get("/benefits", isLoggedIn, benefitsHandler.displayBenefits);` (GET /benefits)
- `app/routes/index.js:56` — `app.post("/benefits", isLoggedIn, benefitsHandler.updateBenefits);` (POST /benefits)
- `app/routes/index.js:58` — `app.get("/benefits", isLoggedIn, isAdmin, benefitsHandler.displayBenefits);` (GET /benefits)
- `app/routes/index.js:59` — `app.post("/benefits", isLoggedIn, isAdmin, benefitsHandler.updateBenefits);` (POST /benefits)

- `app/routes/index.js:63` — `app.get("/allocations/:userId", isLoggedIn, allocationsHandler.displayAllocations);` (GET /allocations/:userId)
- `app/routes/index.js:66` — `app.get("/memos", isLoggedIn, memosHandler.displayMemos);` (GET /memos)
- `app/routes/index.js:67` — `app.post("/memos", isLoggedIn, memosHandler.addMemos);` (POST /memos)
- `app/routes/index.js:70` — `app.get("/learn", isLoggedIn, (req, res) => {` (GET /learn)
- `app/routes/index.js:76` — `app.get("/research", isLoggedIn, researchHandler.displayResearch);` (GET /research)
- `app/routes/tutorial.js:8` — `router.get("/", (req, res) => {` (GET /)
- `app/routes/tutorial.js:31` — `router.get('/${page}', (req, res) => {` (GET /${page})

Oversized functions

`maintainability` · source: scanner (oversized_files) · effort: M · id `0df185b9a631a705`

2 functions are longer than 150 lines; the longest is SessionHandler in app/routes/session.js (268 lines).

Impact. A function this long cannot be unit tested or reasoned about; defects hide in it.

Remediation. Extract cohesive steps into named functions with their own tests.

Effort. M: extract cohesive steps into tested functions (scanner rule oversized_files.function)

Evidence.

- `app/routes/session.js:8-275` (SessionHandler: 268 lines)
- `Gruntfile.js:14-194` (<anonymous>: 181 lines)

Hardcoded URLs

`operability` · source: scanner (hardcoded_infra) · effort: M · id `fbde30d1cd4f9e51`

33 distinct URLs hardcoded at 34 location(s), for example https://github.com/vuejs/vue-router/issues/261, https://raw.github.com/bekk/retire.js/master/repository/jsrepository.json, https://raw.github.com/bekk/retire.js/master/repository/npmrepository.json, https://www.owasp.org/index.php/Projects/OWASP_Node_js_Goat_Project, https://www.owasp.org/skins/owasplogo.png. Showing the first 25 locations.

Impact. Endpoints are fixed in code: moving a service or adding an environment means a code change, and the code reveals where the organisation's systems live.

Remediation. Move these values to configuration (environment variables or a config file) and document each one in the deployment guide.

Effort. M: move the values into configuration per environment (scanner rule hardcoded_infra.url)

Evidence.

- `app/views/tutorial/a8.html:50` — `<form method="POST" action="http://TARGET_APP_URL_HERE/profile">` (value: http://TARGET_APP_URL_HERE/profile)
- `app/views/tutorial/a5.html:50` — `Use latest stable version of node.js and express (or other web framework you are using). Keep a watch on published vulnerabilities of these. The vulnerabilities for node.js and express.js can be found` (value: http://blog.nodejs.org/vulnerability/)
- `app/views/tutorial/a5.html:51` — `<a href="http://expressjs.com/advanced/security-updates.html">here</a>, respectively.` (value: http://expressjs.com/advanced/security-updates.html)
- `app/views/tutorial/a2.html:209` — `<li><a href="http://passportjs.org/guide/authenticate/">Passport</a> authentication middleware</li>` (value: http://passportjs.org/guide/authenticate/)
- `app/views/tutorial/a2.html:207` — `<li><a href="http://recxltd.blogspot.sg/2012/03/seven-web-server-http-headers-that.html">Seven Web Server HTTP Headers that Improve Web Application Security for Free</a>` (value: http://recxltd.blogspot.sg/2012/03/seven-web-server-http-headers-that.html)
- `app/views/tutorial/a9.html:51` — `<a href="https://docs.npmjs.com/cli/v6/commands/npm-outdated">npm outdated</a> and <a href="https://classic.yarnpkg.com/en/docs/cli/outdated">yarn outdated</a> are both command line ways to show possi` (value: https://classic.yarnpkg.com/en/docs/cli/outdated)
- `app/views/tutorial/a9.html:57` — `<a href="https://david-dm.org/">David DM</a> gets you an overview of your project dependencies, the version you use and the latest available, so you can quickly see what's drifting` (value: https://david-dm.org/)
- `app/views/research.html:17` — `<input type="hidden" id="url" name="url" value="https://finance.yahoo.com/quote/"/>` (value: https://finance.yahoo.com/quote/)
- `app/views/tutorial/a9.html:41` — `<a href="https://github.com/advisories">GitHub Advisory Database</a>` (value: https://github.com/advisories)
- `package.json:51` — `"grunt-if": "https://github.com/binarymist/grunt-if/tarball/master",` (value: https://github.com/binarymist/grunt-if/tarball/master)
- `app/views/tutorial/a9.html:113` — `The demo web application is using a popular library called <a href="https://github.com/chjj/marked"> Marked </a> which is a Markdown parser in JavaScript and provides an easy way to integrate markdown` (value: https://github.com/chjj/marked)
- `app/views/tutorial/redos.html:33` — `Use Node.js's <a href="https://github.com/chriso/validator.js/">validator.js</a> package to validate expected data format instead of writing your own regular expressions` (value: https://github.com/chriso/validator.js/)

- `app/views/tutorial/a8.html:59` — `</pre> Note: A sample app containing form for CSRF attack on NodeGoat app is available <a target="_blank" href="https://github.com/ckarande/nodegoat-csrf-attack">here</a>.` (value: https://github.com/ckarande/nodegoat-csrf-attack)
- `app/views/tutorial/redos.html:37` — `<a href="https://github.com/substack/safe-regex">safe-regex</a> package which allows detecting if a regex is prone to catastrophic backtracking, and also allows to configure threshold for maximum repe` (value: https://github.com/substack/safe-regex)
- `Gruntfile.js:105` — `console.log("https://github.com/vuejs/vue-router/issues/261");` (value: https://github.com/vuejs/vue-router/issues/261)
- `app/views/tutorial/a1.html:179` — `<li><a target="_blank" href="https://media.blackhat.com/bh-us-11/Sullivan/BH_US_11_Sullivan_Server_Side_WP.pdf">“ServerSide JavaScript Injection: Attacking NoSQL and Node.js"</a> a whitepaper by Bryan` (value: https://media.blackhat.com/bh-us-11/Sullivan/BH_US_11_Sullivan_Server_Side_WP.pdf)
- `app/views/tutorial/a2.html:206` — `<li><a href="https://npmjs.org/package/helmet">Helmet</a> Security header middleware collection for express</li>` (value: https://npmjs.org/package/helmet)
- `Gruntfile.js:136` — `jsRepository: "https://raw.github.com/bekk/retire.js/master/repository/jsrepository.json",` (value: https://raw.github.com/bekk/retire.js/master/repository/jsrepository.json)
- `Gruntfile.js:137` — `nodeRepository: "https://raw.github.com/bekk/retire.js/master/repository/npmrepository.json",` (value: https://raw.github.com/bekk/retire.js/master/repository/npmrepository.json)
- `app/views/tutorial/a9.html:31` — `<a href="https://snyk.io/">Snyk.io</a> is a Node.js CLI tool and Platform to scan and detect vulnerable packages` (value: https://snyk.io/)
- `app/views/tutorial/a9.html:44` — `<a href="https://snyk.io/vuln">Snyk Vulnerability DB</a>` (value: https://snyk.io/vuln)
- `app/views/layout.html:62` — `<li><a id="learn-menu-link" target="_blank" href="/learn?url=https://www.khanacademy.org/economics-finance-domain/core-finance/investment-vehicles-tutorial/ira-401ks/v/traditional-iras"><i class="fa f` (value: https://www.khanacademy.org/economics-finance-domain/core-finance/investment-vehicles-tutorial/ira-401ks/v/traditional-iras)
- `app/views/tutorial/a5.html:72` — `Lock versions of all npm packages used, for example using <a href="https://www.npmjs.org/doc/cli/npm-shrinkwrap.html"> shrinkwarp</a>, to have full control over when to install a new version of the pa` (value: https://www.npmjs.org/doc/cli/npm-shrinkwrap.html)
- `app/views/tutorial/a3.html:234` — `<a href="https://www.owasp.org/images/c/c5/Unraveling_some_Mysteries_around_DOM-based_XSS.pdf ">Unraveling` (value: https://www.owasp.org/images/c/c5/Unraveling_some_Mysteries_around_DOM-based_XSS.pdf)

- `app.json:9` — `"website": "https://www.owasp.org/index.php/Projects/OWASP_Node_js_Goat_Project",` (value: https://www.owasp.org/index.php/Projects/OWASP_Node_js_Goat_Project)

Hardcoded IP addresses

`operability` · source: scanner (hardcoded_infra) · effort: M · id `cb11e2dae7b2c585`

1 distinct IP addresses hardcoded at 2 location(s), for example 192.168.56.20.

Impact. Fixed addresses break silently when infrastructure moves and expose network layout.

Remediation. Move these values to configuration (environment variables or a config file) and document each one in the deployment guide.

Effort. M: move the values into configuration per environment (scanner rule hardcoded_infra.ip)

Evidence.

- `config/env/development.js:3` — `zapHostName: "192.168.56.20",` (value: 192.168.56.20)
- `config/env/test.js:3` — `zapHostName: "192.168.56.20",` (value: 192.168.56.20)

Known vulnerabilities in ajv 6.10.0

`dependency` · source: scanner (dependencies) · effort: S · id `31bd27cb9bb80b1a`

2 published advisories affect ajv 6.10.0 (npm), declared in package-lock.json: GHSA-2g4f-4pwh-qvx6: ajv has ReDoS when using `$data` option; GHSA-v88g-cgmw-v5xw: Prototype Pollution in Ajv.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade ajv to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-2g4f-4pwh-qvx6, GHSA-v88g-cgmw-v5xw)

Known vulnerabilities in bl 1.0.3

`dependency` · source: scanner (dependencies) · effort: S · id `9234c46543fbd425`

1 published advisory affects bl 1.0.3 (npm), declared in package-lock.json: GHSA-pp7h-53gx-mx7r: Remote Memory Exposure in bl.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade bl to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-pp7h-53gx-mx7r)

Known vulnerabilities in bl 1.1.2

`dependency` · source: scanner (dependencies) · effort: S · id `6fc158a997a3cab6`

1 published advisory affects bl 1.1.2 (npm), declared in package-lock.json: GHSA-pp7h-53gx-mx7r: Remote Memory Exposure in bl.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade bl to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-pp7h-53gx-mx7r)

Known vulnerabilities in express 4.16.4

`dependency` · source: scanner (dependencies) · effort: S · id `080359d31f4d677c`

2 published advisories affect express 4.16.4 (npm), declared in package-lock.json: GHSA-qw6h-vgh9-j6wx: express vulnerable to XSS via response.redirect(); GHSA-rv95-896h-c2vc: Express.js Open Redirect in malformed URLs.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade express to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-qw6h-vgh9-j6wx, GHSA-rv95-896h-c2vc)

Known vulnerabilities in extend 3.0.0

`dependency` · source: scanner (dependencies) · effort: S · id `d79fd8b41579d1e9`

1 published advisory affects extend 3.0.0 (npm), declared in package-lock.json: GHSA-qrmc-fj45-qfc2: Prototype Pollution in extend.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade extend to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-qrmc-fj45-qfc2)

Known vulnerabilities in got 6.7.1

`dependency` · source: scanner (dependencies) · effort: S · id `9c689ad3755fd398`

1 published advisory affects got 6.7.1 (npm), declared in package-lock.json: GHSA-pfrx-2q88-qq97: Got allows a redirect to a UNIX socket.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade got to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-pfrx-2q88-qq97)

Known vulnerabilities in helmet-csp 1.2.2

`dependency` · source: scanner (dependencies) · effort: S · id `eb39c7dbd4067a1d`

1 published advisory affects helmet-csp 1.2.2 (npm), declared in package-lock.json: GHSA-c3m8-x3cg-qm2c: Configuration Override in helmet-csp.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade helmet-csp to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-c3m8-x3cg-qm2c)

Known vulnerabilities in hosted-git-info 2.1.5

`dependency` · source: scanner (dependencies) · effort: S · id `c4b04389367d936b`

1 published advisory affects hosted-git-info 2.1.5 (npm), declared in package-lock.json: GHSA-43f8-2h32-f4cj: Regular Expression Denial of Service in hosted-git-info.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade hosted-git-info to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-43f8-2h32-f4cj)

Known vulnerabilities in hosted-git-info 2.7.1

`dependency` · source: scanner (dependencies) · effort: S · id `7187ceb0062f5b91`

1 published advisory affects hosted-git-info 2.7.1 (npm), declared in package-lock.json: GHSA-43f8-2h32-f4cj: Regular Expression Denial of Service in hosted-git-info.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade hosted-git-info to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-43f8-2h32-f4cj)

Known vulnerabilities in is-my-json-valid 2.15.0

`dependency` · source: scanner (dependencies) · effort: S · id `7feeaaa5fcaea64f`

1 published advisory affects is-my-json-valid 2.15.0 (npm), declared in package-lock.json: GHSA-4hpf-3wq7-5rpr: Regular expression deinal of service (ReDoS) in is-my-json-valid.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade is-my-json-valid to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-4hpf-3wq7-5rpr)

Known vulnerabilities in jsonpointer 4.0.0

`dependency` · source: scanner (dependencies) · effort: S · id `68cb97edadbae3e4`

1 published advisory affects jsonpointer 4.0.0 (npm), declared in package-lock.json: GHSA-282f-qqgm-c34q: Prototype Pollution in node-jsonpointer.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade jsonpointer to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-282f-qqgm-c34q)

Known vulnerabilities in jsonpointer 4.0.1

`dependency` · source: scanner (dependencies) · effort: S · id `f3f0f9554cfc21e9`

1 published advisory affects jsonpointer 4.0.1 (npm), declared in package-lock.json: GHSA-282f-qqgm-c34q: Prototype Pollution in node-jsonpointer.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade jsonpointer to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-282f-qqgm-c34q)

Known vulnerabilities in micromatch 2.3.11

`dependency` · source: scanner (dependencies) · effort: S · id `13cd3faa49512d1a`

1 published advisory affects micromatch 2.3.11 (npm), declared in package-lock.json: GHSA-952p-6rrq-rcjv: Regular Expression Denial of Service (ReDoS) in micromatch.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade micromatch to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-952p-6rrq-rcjv)

Known vulnerabilities in micromatch 3.1.10

`dependency` · source: scanner (dependencies) · effort: S · id `7fe16fadabfe99d5`

1 published advisory affects micromatch 3.1.10 (npm), declared in package-lock.json: GHSA-952p-6rrq-rcjv: Regular Expression Denial of Service (ReDoS) in micromatch.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade micromatch to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-952p-6rrq-rcjv)

Known vulnerabilities in ms 0.7.1

`dependency` · source: scanner (dependencies) · effort: S · id `5451bdfe48777b5f`

1 published advisory affects ms 0.7.1 (npm), declared in package-lock.json: GHSA-w9mr-4mfr-499f: Vercel ms Inefficient Regular Expression Complexity vulnerability.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade ms to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-w9mr-4mfr-499f)

Known vulnerabilities in path-parse 1.0.5

`dependency` · source: scanner (dependencies) · effort: S · id `80bd8a4e2f31f886`

1 published advisory affects path-parse 1.0.5 (npm), declared in package-lock.json: GHSA-hj48-42vr-x3v9: Regular Expression Denial of Service in path-parse.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade path-parse to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-hj48-42vr-x3v9)

Known vulnerabilities in randomatic 1.1.5

`dependency` · source: scanner (dependencies) · effort: S · id `abac730967770e4a`

1 published advisory affects randomatic 1.1.5 (npm), declared in package-lock.json: GHSA-6g33-f262-xjp4: Cryptographically Weak PRNG in randomatic.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade randomatic to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-6g33-f262-xjp4)

Known vulnerabilities in request 2.36.0

`dependency` · source: scanner (dependencies) · effort: S · id `076535a3b988e108`

2 published advisories affect request 2.36.0 (npm), declared in package-lock.json: GHSA-7xfp-9c55-5vqj: Remote Memory Exposure in request; GHSA-p8p7-x288-28g6: Server-Side Request Forgery in Request.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade request to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-7xfp-9c55-5vqj, GHSA-p8p7-x288-28g6)

Known vulnerabilities in request 2.67.0

`dependency` · source: scanner (dependencies) · effort: S · id `b4925464ab8f8813`

2 published advisories affect request 2.67.0 (npm), declared in package-lock.json: GHSA-7xfp-9c55-5vqj: Remote Memory Exposure in request; GHSA-p8p7-x288-28g6: Server-Side Request Forgery in Request.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade request to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-7xfp-9c55-5vqj, GHSA-p8p7-x288-28g6)

Known vulnerabilities in request 2.75.0

`dependency` · source: scanner (dependencies) · effort: S · id `036848d6f6a3675a`

1 published advisory affects request 2.75.0 (npm), declared in package-lock.json: GHSA-p8p7-x288-28g6: Server-Side Request Forgery in Request.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade request to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-p8p7-x288-28g6)

Known vulnerabilities in request 2.79.0

`dependency` · source: scanner (dependencies) · effort: S · id `a2ec2c2045122038`

1 published advisory affects request 2.79.0 (npm), declared in package-lock.json: GHSA-p8p7-x288-28g6: Server-Side Request Forgery in Request.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade request to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-p8p7-x288-28g6)

Known vulnerabilities in request 2.88.0

`dependency` · source: scanner (dependencies) · effort: S · id `6f4156345bf302e7`

1 published advisory affects request 2.88.0 (npm), declared in package-lock.json: GHSA-p8p7-x288-28g6: Server-Side Request Forgery in Request.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade request to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-p8p7-x288-28g6)

Known vulnerabilities in send 0.16.2

`dependency` · source: scanner (dependencies) · effort: S · id `c0b2917d05787a53`

1 published advisory affects send 0.16.2 (npm), declared in package-lock.json: GHSA-m6fv-jmcg-4jfg: send vulnerable to template injection that can lead to XSS.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade send to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-m6fv-jmcg-4jfg)

Known vulnerabilities in serve-static 1.13.2

`dependency` · source: scanner (dependencies) · effort: S · id `84eec6fe5da6d12e`

1 published advisory affects serve-static 1.13.2 (npm), declared in package-lock.json: GHSA-cm22-4g7w-348p: serve-static vulnerable to template injection that can lead to XSS.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade serve-static to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-cm22-4g7w-348p)

Known vulnerabilities in stringstream 0.0.5

`dependency` · source: scanner (dependencies) · effort: S · id `5fba0d8cf32f9f52`

1 published advisory affects stringstream 0.0.5 (npm), declared in package-lock.json: GHSA-mf6x-7mm4-x2g7: Out-of-bounds Read in stringstream.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade stringstream to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-mf6x-7mm4-x2g7)

Known vulnerabilities in tough-cookie 2.3.4

`dependency` · source: scanner (dependencies) · effort: S · id `6abd3656aeac5d20`

1 published advisory affects tough-cookie 2.3.4 (npm), declared in package-lock.json: GHSA-72xf-g2v4-qvf3: tough-cookie Prototype Pollution vulnerability.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade tough-cookie to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-72xf-g2v4-qvf3)

Known vulnerabilities in tough-cookie 2.4.3

`dependency` · source: scanner (dependencies) · effort: S · id `2d7bf77028306507`

1 published advisory affects tough-cookie 2.4.3 (npm), declared in package-lock.json: GHSA-72xf-g2v4-qvf3: tough-cookie Prototype Pollution vulnerability.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade tough-cookie to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-72xf-g2v4-qvf3)

Known vulnerabilities in tunnel-agent 0.4.3

`dependency` · source: scanner (dependencies) · effort: S · id `8beaf39971051c60`

1 published advisory affects tunnel-agent 0.4.3 (npm), declared in package-lock.json: GHSA-xc7v-wxcw-j472: Memory Exposure in tunnel-agent.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade tunnel-agent to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-xc7v-wxcw-j472)

Known vulnerabilities in undefsafe 2.0.2

`dependency` · source: scanner (dependencies) · effort: S · id `f7411d9164a0fb35`

1 published advisory affects undefsafe 2.0.2 (npm), declared in package-lock.json: GHSA-332q-7ff2-57h2: Prototype Pollution in undefsafe.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade undefsafe to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-332q-7ff2-57h2)

Known vulnerabilities in xml2js 0.4.4

`dependency` · source: scanner (dependencies) · effort: S · id `ef60942483830d38`

1 published advisory affects xml2js 0.4.4 (npm), declared in package-lock.json: GHSA-776f-qx25-q3cc: xml2js is vulnerable to prototype pollution.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade xml2js to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-776f-qx25-q3cc)

Known vulnerabilities in yargs-parser 2.4.1

`dependency` · source: scanner (dependencies) · effort: S · id `87dbd776b62dadf7`

1 published advisory affects yargs-parser 2.4.1 (npm), declared in package-lock.json: GHSA-p9pc-299p-vxgp: yargs-parser Vulnerable to Prototype Pollution.

Impact. The tool ships a dependency with publicly documented weaknesses; exploit details for published advisories are usually available.

Remediation. Upgrade yargs-parser to a release that fixes these advisories, then re-run the scan. Check the advisories for configuration workarounds if an upgrade must wait.

Effort. S: upgrade the package; more across a major version (scanner rule dependencies.advisories)

Evidence.

- `package-lock.json` (advisories: GHSA-p9pc-299p-vxgp)

Low (7)

One row per finding. Impact, remediation, and excerpts for each are in `analysis/findings.json`, and `unvarnish ask` can explain any of them.

Finding	Category	Source	Effort	Location
No linter or formatter configuration	maintainability	scanner	S	`.`
Known vulnerabilities in chownr 1.0.1	dependency	scanner	S	`package-lock.json`
Known vulnerabilities in cookie 0.3.1	dependency	scanner	S	`package-lock.json`
Known vulnerabilities in debug 3.2.6	dependency	scanner	S	`package-lock.json`
Known vulnerabilities in debug 4.1.1	dependency	scanner	S	`package-lock.json`
Known vulnerabilities in es5-ext 0.10.12	dependency	scanner	S	`package-lock.json`
Known vulnerabilities in on-headers 1.0.1	dependency	scanner	S	`package-lock.json`

Not analysed

Excluded from analysis but counted in totals:

- **lockfile**: 1 file(s) — e.g. `package-lock.json`
- **vendored:vendor**: 15 file(s) — e.g. `app/assets/vendor/bootstrap/bootstrap-tour.css`, `app/assets/vendor/bootstrap/bootstrap-tour.js`, `app/assets/vendor/bootstrap/bootstrap.css`, `app/assets/vendor/bootstrap/bootstrap.js`, `app/assets/vendor/chart/morris-0.4.3.min.js`

Binary files (3): `app/assets/favicon.ico`, `app/assets/images/nodegoat_logo.png`, `app/assets/images/owasplogo.png`

Hardcoded-infrastructure scanning reads the first 4,000 characters of each line.