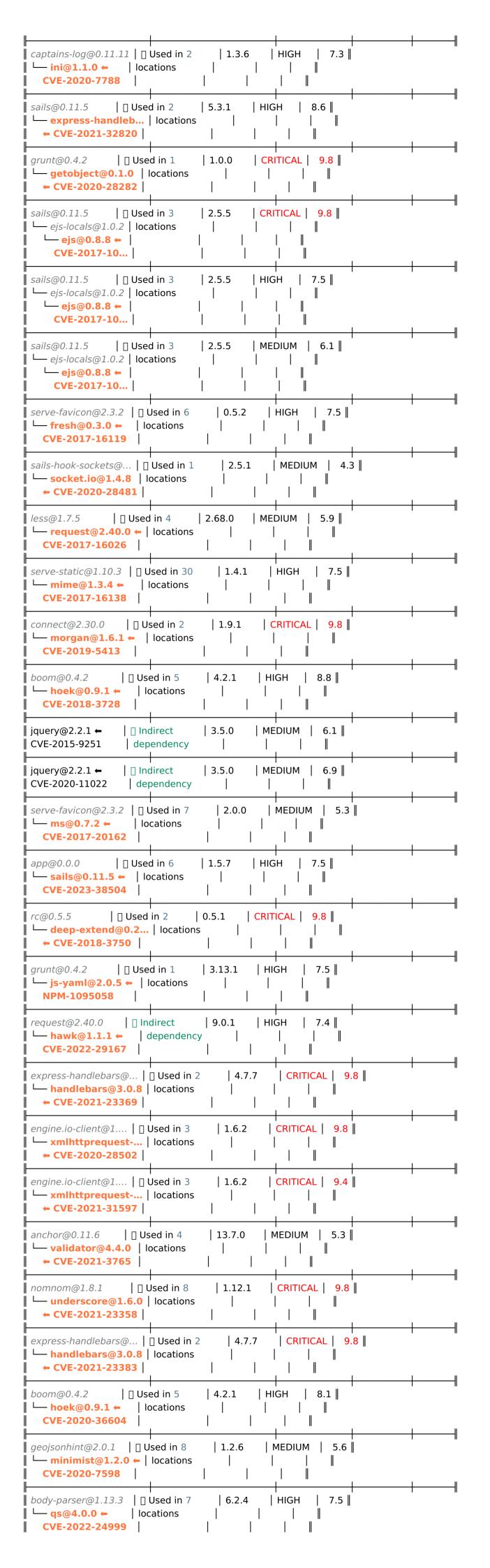
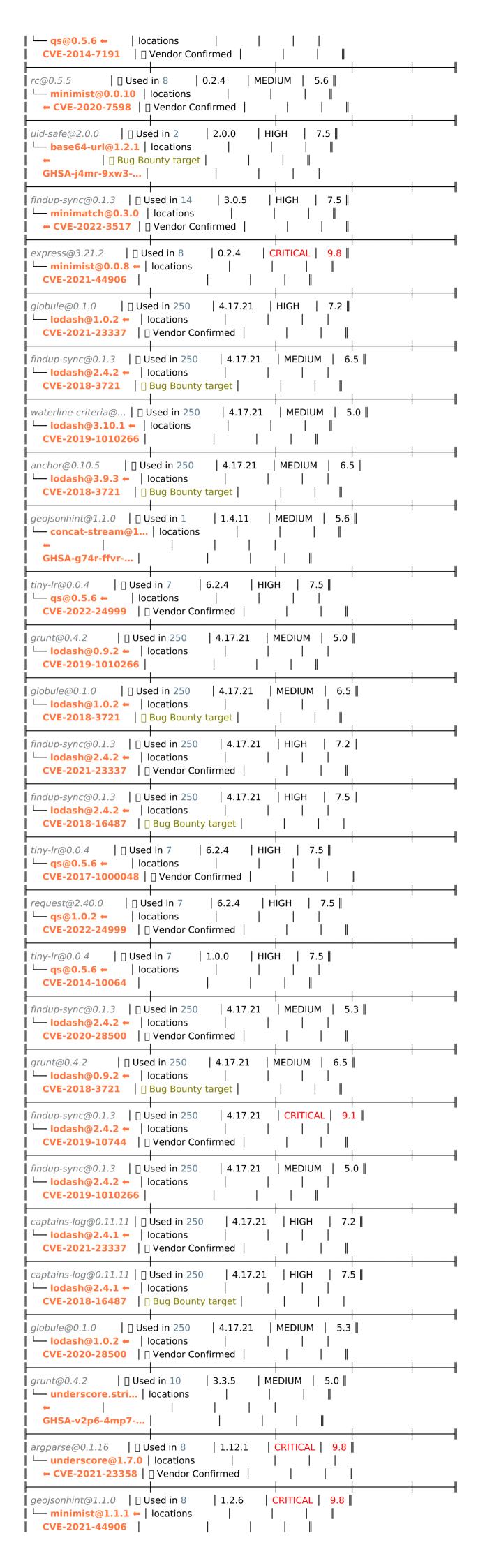
Dependency Scan Results (JS)

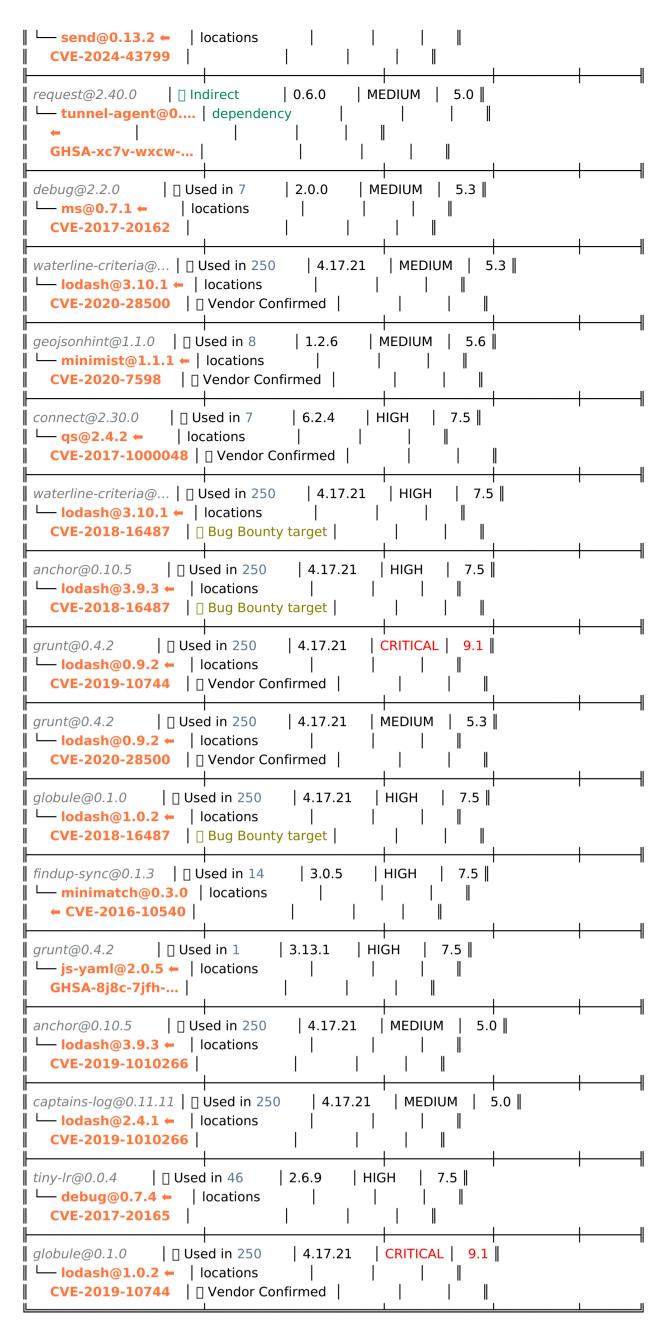
Dependency Scan Results (JS)	
Dependency Tree Insights Fix Version Severity Score	
sails-generate-cont □ Used in 10 3.3.5 MEDIUM 5.0	——
grunt@0.4.2	
request@2.40.0	
jsonwebtoken@4.0.0	
body-parser@1.13.3 □ Used in 7 6.2.4 HIGH 7.5	
express-handlebars@ □ Used in 2 4.7.7 MEDIUM 6.1	
app@0.0.0	
app@0.0.0	
sails@0.11.5	—
socket.io@1.4.8	——
socket.io@1.4.8	
socket.io-client@1 □ Used in 7 3.3.4 HIGH 7.5	
grunt-contrib-clean □ Used in 1 1.5.3 HIGH 7.1	
vfile-reporter@3.0.0 □ Used in 1 0.0.3 HIGH 7.5	
sails@0.11.5	—
engine.io-client@1 □ Used in 1	—
uid-safe@2.0.0	
engine.io-client@1 □ Used in 2	
app@0.0.0	——II
engine.io@1.6.11	——II
engine.io-client@1 □ Used in 2	
grunt-contrib-clean □ Used in 1 1.5.3 HIGH 7.0 □ grunt@0.4.2 ← locations CVE-2022-1537	
grunt-contrib-clean □ Used in 1 1.5.3 MEDIUM 5.5	—— "
	 -
request@2.40.0	
jwa@1.0.2	—-



sails@0.11.5
socket.io-client@1 □ Used in 7 3.3.4 CRITICAL 9.8 Socket.io-parse locations ← CVE-2022-2421
jquery@2.2.1 ← □ Indirect 3.5.0 MEDIUM 6.9
geojsonhint@2.0.1 □ Used in 8 1.2.6 CRITICAL 9.8
app@0.0.0
app@0.0.0
app@0.0.0
socket.io-client@1 □ Used in 7 3.3.4 HIGH 7.3
sails@0.11.5
sails-hook-sockets@ □ Used in 1 2.5.1 HIGH 7.3
skipper@0.5.9
connect@2.30.0
express@3.21.2
connect@2.30.0
sails@0.11.5
jwa@1.0.2
GHSA-rvg8-pwq2
jws@2.0.0
waterline-criteria@ □ Used in 250 4.17.21 MEDIUM 6.5
anchor@0.10.5
argparse@0.1.16
GHSA-v2p6-4mp7
captains-log@0.11.11 □ Used in 250 4.17.21 CRITICAL 9.1
tiny-lr@0.0.4



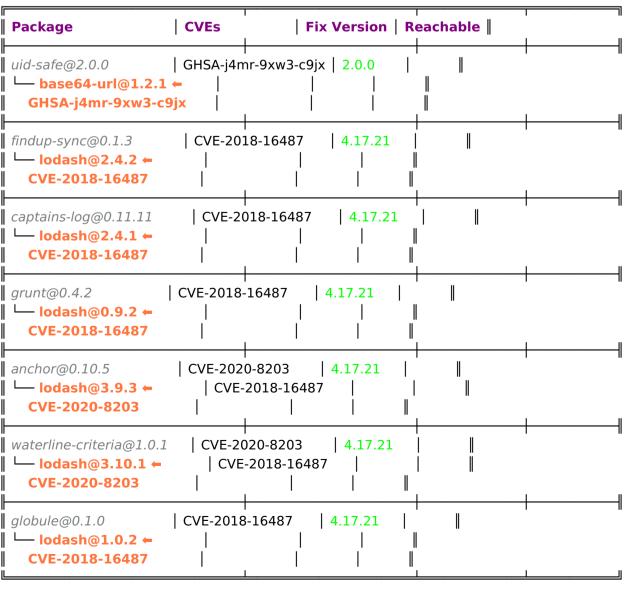
<u> </u>
request@2.40.0 □ Used in 7 6.2.4 HIGH 7.5 □ qs@1.0.2 ← locations CVE-2017-1000048 □ Vendor Confirmed
socket.io-adapter@0 □ Used in 7 3.3.4 HIGH 7.5
captains-log@0.11.11 □ Used in 250 4.17.21 MEDIUM 5.3 □ lodash@2.4.1 ← locations CVE-2020-28500 □ Vendor Confirmed
include-all@0.1.6 ☐ Used in 10 3.3.5 MEDIUM 5.0
GHSA-v2p6-4mp7
anchor@0.10.5 ☐ Used in 4 13.7.0 MEDIUM 5.3 — validator@3.41.2 locations ← CVE-2021-3765 ☐ Bug Bounty target
anchor@0.10.5 □ Used in 250 4.17.21 HIGH 7.2 Lodash@3.9.3 ← locations CVE-2021-23337 □ Vendor Confirmed
engine.io-client@1 ☐ Used in 2
anchor@0.10.5 □ Used in 250 4.17.21 CRITICAL 9.1
waterline-criteria@ □ Used in 250 4.17.21 CRITICAL 9.1 Lodash@3.10.1 ← locations CVE-2019-10744 □ Vendor Confirmed
connect@2.30.0 □ Used in 7 6.2.4 HIGH 7.5 □ qs@2.4.2 ← locations CVE-2022-24999 □ Vendor Confirmed
grunt@0.4.2 □ Used in 1 3.13.1 MEDIUM 5.9 js-yaml@2.0.5 ← locations GHSA-2pr6-76vf
body-parser@1.13.3 □ Used in 46 2.6.9 HIGH 7.5 □ debug@2.2.0 ← locations CVE-2017-20165
grunt@0.4.2 □ Used in 250 4.17.21 HIGH 7.5 Lodash@0.9.2 ← locations CVE-2018-16487 Bug Bounty target
waterline-criteria@ □ Used in 250 4.17.21 HIGH 7.2 □ lodash@3.10.1 ← locations CVE-2021-23337 □ Vendor Confirmed
accepts@1.2.13
anchor@0.10.5 □ Used in 250 4.17.21 HIGH 7.4 □ lodash@3.9.3 ← locations CVE-2020-8203 □ Bug Bounty target
engine.io@1.6.11 ☐ Used in 2 1.1.5 HIGH 7.5 — ws@1.1.0 ← locations
form-data@0.1.4 □ Used in 30 1.4.1 HIGH 7.5 □ mime@1.2.11 ← locations
waterline-criteria@ □ Used in 250 4.17.21 HIGH 7.4 Lodash@3.10.1 ← locations CVE-2020-8203 □ Bug Bounty target
engine.io@1.6.11
glob@3.1.21
glob@3.1.21 □ Used in 14 3.0.5 HIGH 7.5 minimatch@0.2.14 locations ← CVE-2022-3517 □ Vendor Confirmed
sails-generate-cont □ Used in 10 3.3.5 MEDIUM 5.0 underscore.stri locations GHSA-v2p6-4mp7
grunt@0.4.2 □ Used in 250 4.17.21 HIGH 7.2 □ lodash@0.9.2 ← locations CVE-2021-23337 □ Vendor Confirmed
rc@0.5.5
socket.io-adapter@0 □ Used in 7 3.3.4 HIGH 7.3 socket.io-parse locations ← CVE-2023-32695



Next Steps

Below are the vulnerabilities prioritized by depscan. Follow your team's remediation workflow to mitigate these findings.

Top Priority (JS)



Recommendation

You can remediate 91 vulnerabilities by updating the packages using the fix

☐ 89 out of 153 vulnerabilities requires your attention.

version 🛚