

























































Risk Audit Capability

Depscan supports OSS Risk audit for this project.

To enable set the environment variable **ENABLE_OSS_RISK=true**

Dependency Scan Results (JS)				
Dependency Tree	Insights	Fix Version	Severity	Score
sails-generate-cont... └─ underscore.stri... ↪ NPM-1085693	Used in 10 locations	3.3.5	MEDIUM	5.0
grunt@0.4.2 └─ js-yaml@2.0.5 ↪ NPM-1085724	Used in 1 locations	3.13.1	MEDIUM	5.9
request@2.40.0 └─ tunnel-agent@0.... ↪ NPM-1085744	Indirect dependency	0.6.0	MEDIUM	5.0
jsonwebtoken@4.0.0 └─ jws@2.0.0 ↪ CVE-2016-1000223	Used in 1 locations	3.0.0	HIGH	8.7
body-parser@1.13.3 └─ qs@4.0.0 ↪ CVE-2017-1000048	Used in 7 locations	6.2.4	HIGH	7.5
express-handlebars@... └─ handlebars@3.0.8 ↪ CVE-2015-8861	Used in 2 locations	4.7.7	MEDIUM	6.1
app@0.0.0 └─ sails@0.11.5 ↪ CVE-2016-10549	Used in 6 locations	0.12.7	HIGH	7.5
app@0.0.0 └─ sails@0.11.5 ↪ CVE-2021-44908	Used in 6 locations	1.5.7	CRITICAL	9.8
sails@0.11.5 └─ ejs-locals@1.0.2 └─ ejs@0.8.8 ↪ CVE-2022-29...	Used in 3 locations	3.1.10	CRITICAL	9.8
socket.io@1.4.8 └─ engine.io@1.6.11 ↪ CVE-2020-36048	Used in 1 locations	3.6.1	HIGH	7.5
socket.io@1.4.8 └─ engine.io@1.6.11 ↪ CVE-2022-41940	Used in 1 locations	3.6.1	MEDIUM	6.5
socket.io-client@1.... └─ socket.io-parse... ↪ CVE-2020-36049	Used in 7 locations	3.3.4	HIGH	7.5
grunt-contrib-clean... └─ grunt@0.4.2 ↪ CVE-2020-7729	Used in 1 locations	1.5.3	HIGH	7.1
vfile-reporter@3.0.0 └─ trim@0.0.1 ↪ CVE-2020-7753	Used in 1 locations	0.0.3	HIGH	7.5
sails@0.11.5 └─ sails-hook-sock... ↪ CVE-2018-21036	Indirect dependency	1.5.5	HIGH	7.5
engine.io-client@1.... └─ parsejson@0.0.1 ↪ CVE-2017-16113	Used in 1 locations		HIGH	7.5
uid-safe@2.0.0 └─ base64-url@1.2.1 ↪ NPM-1090859	Used in 2 locations	2.0.0	HIGH	7.5
engine.io-client@1.... └─ ws@1.0.1 ↪ CVE-2016-10542	Used in 2 locations	1.1.5	HIGH	7.5
app@0.0.0 └─ jsonwebtoken@4.... ↪ CVE-2015-9235	Used in 4 locations	4.2.2	CRITICAL	9.0
engine.io@1.6.11 └─ negotiator@0.4.9 ↪ CVE-2016-10539	Used in 3 locations	0.6.1	HIGH	7.5
engine.io-client@1.... └─ ws@1.0.1 ↪ NPM-1091478	Used in 2 locations	1.1.5	HIGH	7.5
grunt-contrib-clean... └─ grunt@0.4.2 ↪ CVE-2022-1537	Used in 1 locations	1.5.3	HIGH	7.0
grunt-contrib-clean... └─ grunt@0.4.2 ↪ CVE-2022-0436	Used in 1 locations	1.5.3	MEDIUM	5.5
less@1.7.5 └─ clean-css@2.2.23 ↪ NPM-1091669	Used in 24 locations	4.1.11	LOW	2.0
request@2.40.0 └─ hawk@1.1.1 ↪ CVE-2016-2515	Indirect dependency	3.1.3	HIGH	7.5
jwa@1.0.2 └─ base64url@0.0.6 ↪ NPM-1091792	Used in 3 locations	3.0.0	MEDIUM	5.0

captains-log@0.11.11  Used in 2 1.3.6 HIGH 7.3									
└─ ini@1.1.0  locations									
CVE-2020-7788									
sails@0.11.5  Used in 2 5.3.1 HIGH 8.6									
└─ express-handleb... locations									
 CVE-2021-32820									
grunt@0.4.2  Used in 1 1.0.0 CRITICAL 9.8									
└─ getobject@0.1.0 locations									
 CVE-2020-28282									
sails@0.11.5  Used in 3 2.5.5 CRITICAL 9.8									
└─ ejs-locals@1.0.2 locations									
└─ ejs@0.8.8 									
CVE-2017-10...									
sails@0.11.5  Used in 3 2.5.5 HIGH 7.5									
└─ ejs-locals@1.0.2 locations									
└─ ejs@0.8.8 									
CVE-2017-10...									
sails@0.11.5  Used in 3 2.5.5 MEDIUM 6.1									
└─ ejs-locals@1.0.2 locations									
└─ ejs@0.8.8 									
CVE-2017-10...									
serve-favicon@2.3.2  Used in 6 0.5.2 HIGH 7.5									
└─ fresh@0.3.0  locations									
CVE-2017-16119									
sails-hook-sockets@...  Used in 1 2.5.1 MEDIUM 4.3									
└─ socket.io@1.4.8 locations									
 CVE-2020-28481									
less@1.7.5  Used in 4 2.68.0 MEDIUM 5.9									
└─ request@2.40.0  locations									
CVE-2017-16026									
serve-static@1.10.3  Used in 30 1.4.1 HIGH 7.5									
└─ mime@1.3.4  locations									
CVE-2017-16138									
connect@2.30.0  Used in 2 1.9.1 CRITICAL 9.8									
└─ morgan@1.6.1  locations									
CVE-2019-5413									
boom@0.4.2  Used in 5 4.2.1 HIGH 8.8									
└─ hoek@0.9.1  locations									
CVE-2018-3728									
jquery@2.2.1   Indirect 3.5.0 MEDIUM 6.1									
CVE-2015-9251 dependency									
jquery@2.2.1   Indirect 3.5.0 MEDIUM 6.9									
CVE-2020-11022 dependency									
serve-favicon@2.3.2  Used in 7 2.0.0 MEDIUM 5.3									
└─ ms@0.7.2  locations									
CVE-2017-20162									
app@0.0.0  Used in 6 1.5.7 HIGH 7.5									
└─ sails@0.11.5  locations									
CVE-2023-38504									
rc@0.5.5  Used in 2 0.5.1 CRITICAL 9.8									
└─ deep-extend@0.2... locations									
 CVE-2018-3750									
grunt@0.4.2  Used in 1 3.13.1 HIGH 7.5									
└─ js-yaml@2.0.5  locations									
NPM-1095058									
request@2.40.0  Indirect 9.0.1 HIGH 7.4									
└─ hawk@1.1.1  dependency									
CVE-2022-29167									
express-handlebars@...  Used in 2 4.7.7 CRITICAL 9.8									
└─ handlebars@3.0.8 locations									
 CVE-2021-23369									
engine.io-client@1....  Used in 3 1.6.2 CRITICAL 9.8									
└─ xmlhttprequest-... locations									
 CVE-2020-28502									
engine.io-client@1....  Used in 3 1.6.2 CRITICAL 9.4									
└─ xmlhttprequest-... locations									
 CVE-2021-31597									
anchor@0.11.6  Used in 4 13.7.0 MEDIUM 5.3									
└─ validator@4.4.0 locations									
 CVE-2021-3765									
nomnom@1.8.1  Used in 8 1.12.1 CRITICAL 9.8									
└─ underscore@1.6.0 locations									
 CVE-2021-23358									
express-handlebars@...  Used in 2 4.7.7 CRITICAL 9.8									
└─ handlebars@3.0.8 locations									
 CVE-2021-23383									
boom@0.4.2  Used in 5 4.2.1 HIGH 8.1									
└─ hoek@0.9.1  locations									
CVE-2020-36604									
geojsonhint@2.0.1  Used in 8 1.2.6 MEDIUM 5.6									
└─ minimist@1.2.0  locations									
CVE-2020-7598									
body-parser@1.13.3  Used in 7 6.2.4 HIGH 7.5									
└─ qs@4.0.0  locations									
CVE-2022-24999									

<div>less@1.7.5</div> <div>request@2.40.0 ← CVE-2023-28155</div> <div>Used in 4 locations</div> <div>2.68.0</div> <div>MEDIUM</div> <div>6.1</div>	
<div>sails@0.11.5</div> <div>express@3.21.2 ← CVE-2024-29041</div> <div>Used in 10 locations</div> <div>4.20.0</div> <div>MEDIUM</div> <div>6.1</div>	
<div>socket.io-client@1....</div> <div>socket.io-parse... ← CVE-2022-2421</div> <div>Used in 7 locations</div> <div>3.3.4</div> <div>CRITICAL</div> <div>9.8</div>	
<div>jquery@2.2.1 ← CVE-2019-11358</div> <div>Indirect dependency</div> <div>3.5.0</div> <div>MEDIUM</div> <div>6.1</div>	
<div>jquery@2.2.1 ← CVE-2020-11023</div> <div>Indirect dependency</div> <div>3.5.0</div> <div>MEDIUM</div> <div>6.9</div>	
<div>geojsonhint@2.0.1</div> <div>minimist@1.2.0 ← CVE-2021-44906</div> <div>Used in 8 locations</div> <div>1.2.6</div> <div>CRITICAL</div> <div>9.8</div>	
<div>app@0.0.0</div> <div>jsonwebtoken@4.... ← CVE-2022-23540</div> <div>Used in 4 locations</div> <div>9.0.0</div> <div>MEDIUM</div> <div>6.4</div>	
<div>app@0.0.0</div> <div>jsonwebtoken@4.... ← CVE-2022-23539</div> <div>Used in 4 locations</div> <div>9.0.0</div> <div>HIGH</div> <div>8.1</div>	
<div>app@0.0.0</div> <div>jsonwebtoken@4.... ← CVE-2022-23541</div> <div>Used in 4 locations</div> <div>9.0.0</div> <div>MEDIUM</div> <div>5.0</div>	
<div>socket.io-client@1....</div> <div>socket.io-parse... ← CVE-2023-32695</div> <div>Used in 7 locations</div> <div>3.3.4</div> <div>HIGH</div> <div>7.3</div>	
<div>sails@0.11.5</div> <div>ejs-locals@1.0.2</div> <div>ejs@0.8.8 ← CVE-2024-33...</div> <div>Used in 3 locations</div> <div>3.1.10</div> <div>MEDIUM</div> <div>4.0</div>	
<div>sails-hook-sockets@...</div> <div>socket.io@1.4.8 ← CVE-2024-38355</div> <div>Used in 1 locations</div> <div>2.5.1</div> <div>HIGH</div> <div>7.3</div>	
<div>skipper@0.5.9</div> <div>semver@5.0.3 ← CVE-2022-25883</div> <div>Used in 5 locations</div> <div>5.7.2</div> <div>HIGH</div> <div>7.5</div>	
<div>connect@2.30.0</div> <div>body-parser@1.1... ← CVE-2024-45590</div> <div>Used in 5 locations</div> <div>1.20.3</div> <div>HIGH</div> <div>7.5</div>	
<div>express@3.21.2</div> <div>send@0.13.0 ← CVE-2024-43799</div> <div>Used in 2 locations</div> <div>0.19.0</div> <div>MEDIUM</div> <div>5.0</div>	
<div>connect@2.30.0</div> <div>serve-static@1.... ← CVE-2024-43800</div> <div>Used in 2 locations</div> <div>1.16.0</div> <div>MEDIUM</div> <div>5.0</div>	
<div>sails@0.11.5</div> <div>express@3.21.2 ← CVE-2024-43796</div> <div>Used in 10 locations</div> <div>4.20.0</div> <div>MEDIUM</div> <div>5.0</div>	
<div>less@1.7.5</div> <div>clean-css@2.2.23 ← GHSA-wxhq-pm8v-...</div> <div>Used in 24 locations</div> <div>4.1.11</div> <div>LOW</div> <div>2.0</div>	
<div>jwa@1.0.2</div> <div>base64url@0.0.6 ← GHSA-rvg8-pwq2-...</div> <div>Used in 3 locations</div> <div>3.0.0</div> <div>MEDIUM</div> <div>5.0</div>	<div>Bug Bounty target</div>
<div>globule@0.1.0</div> <div>lodash@1.0.2 ← CVE-2019-1010266</div> <div>Used in 250 locations</div> <div>4.17.21</div> <div>MEDIUM</div> <div>5.0</div>	
<div>captains-log@0.11.11</div> <div>lodash@2.4.1 ← CVE-2018-3721</div> <div>Used in 250 locations</div> <div>4.17.21</div> <div>MEDIUM</div> <div>6.5</div>	<div>Bug Bounty target</div>
<div>jws@2.0.0</div> <div>base64url@1.0.6 ← GHSA-rvg8-pwq2-...</div> <div>Used in 3 locations</div> <div>3.0.0</div> <div>MEDIUM</div> <div>5.0</div>	<div>Bug Bounty target</div>
<div>waterline-criteria@...</div> <div>lodash@3.10.1 ← CVE-2018-3721</div> <div>Used in 250 locations</div> <div>4.17.21</div> <div>MEDIUM</div> <div>6.5</div>	<div>Bug Bounty target</div>
<div>anchor@0.10.5</div> <div>lodash@3.9.3 ← CVE-2020-28500</div> <div>Used in 250 locations</div> <div>4.17.21</div> <div>MEDIUM</div> <div>5.3</div>	<div>Vendor Confirmed</div>
<div>argparse@0.1.16</div> <div>underscore.stri... ← GHSA-v2p6-4mp7-...</div> <div>Used in 10 locations</div> <div>3.3.5</div> <div>MEDIUM</div> <div>5.0</div>	
<div>express@3.21.2</div> <div>minimist@0.0.8 ← CVE-2020-7598</div> <div>Used in 8 locations</div> <div>0.2.4</div> <div>MEDIUM</div> <div>5.6</div>	<div>Vendor Confirmed</div>
<div>captains-log@0.11.11</div> <div>lodash@2.4.1 ← CVE-2019-10744</div> <div>Used in 250 locations</div> <div>4.17.21</div> <div>CRITICAL</div> <div>9.1</div>	<div>Vendor Confirmed</div>
<div>tiny-lr@0.0.4</div> <div></div> <div>Used in 7 locations</div> <div>1.0.0</div> <div>HIGH</div> <div>7.5</div>	

└─ qs@0.5.6 ←	locations				
CVE-2014-7191	□ Vendor Confirmed				
rc@0.5.5	□ Used in 8	0.2.4	MEDIUM	5.6	
└─ minimist@0.0.10	locations				
← CVE-2020-7598	□ Vendor Confirmed				
uid-safe@2.0.0	□ Used in 2	2.0.0	HIGH	7.5	
└─ base64-url@1.2.1	locations				
←	□ Bug Bounty target				
GHSA-j4mr-9xw3-...					
findup-sync@0.1.3	□ Used in 14	3.0.5	HIGH	7.5	
└─ minimatch@0.3.0	locations				
← CVE-2022-3517	□ Vendor Confirmed				
express@3.21.2	□ Used in 8	0.2.4	CRITICAL	9.8	
└─ minimist@0.0.8 ←	locations				
CVE-2021-44906					
globule@0.1.0	□ Used in 250	4.17.21	HIGH	7.2	
└─ lodash@1.0.2 ←	locations				
CVE-2021-23337	□ Vendor Confirmed				
findup-sync@0.1.3	□ Used in 250	4.17.21	MEDIUM	6.5	
└─ lodash@2.4.2 ←	locations				
CVE-2018-3721	□ Bug Bounty target				
waterline-criteria@...	□ Used in 250	4.17.21	MEDIUM	5.0	
└─ lodash@3.10.1 ←	locations				
CVE-2019-1010266					
anchor@0.10.5	□ Used in 250	4.17.21	MEDIUM	6.5	
└─ lodash@3.9.3 ←	locations				
CVE-2018-3721	□ Bug Bounty target				
geojsonhint@1.1.0	□ Used in 1	1.4.11	MEDIUM	5.6	
└─ concat-stream@1...	locations				
←					
GHSA-g74r-ffvr-...					
tiny-lr@0.0.4	□ Used in 7	6.2.4	HIGH	7.5	
└─ qs@0.5.6 ←	locations				
CVE-2022-24999	□ Vendor Confirmed				
grunt@0.4.2	□ Used in 250	4.17.21	MEDIUM	5.0	
└─ lodash@0.9.2 ←	locations				
CVE-2019-1010266					
globule@0.1.0	□ Used in 250	4.17.21	MEDIUM	6.5	
└─ lodash@1.0.2 ←	locations				
CVE-2018-3721	□ Bug Bounty target				
findup-sync@0.1.3	□ Used in 250	4.17.21	HIGH	7.2	
└─ lodash@2.4.2 ←	locations				
CVE-2021-23337	□ Vendor Confirmed				
findup-sync@0.1.3	□ Used in 250	4.17.21	HIGH	7.5	
└─ lodash@2.4.2 ←	locations				
CVE-2018-16487	□ Bug Bounty target				
tiny-lr@0.0.4	□ Used in 7	6.2.4	HIGH	7.5	
└─ qs@0.5.6 ←	locations				
CVE-2017-1000048	□ Vendor Confirmed				
request@2.40.0	□ Used in 7	6.2.4	HIGH	7.5	
└─ qs@1.0.2 ←	locations				
CVE-2022-24999	□ Vendor Confirmed				
tiny-lr@0.0.4	□ Used in 7	1.0.0	HIGH	7.5	
└─ qs@0.5.6 ←	locations				
CVE-2014-10064					
findup-sync@0.1.3	□ Used in 250	4.17.21	MEDIUM	5.3	
└─ lodash@2.4.2 ←	locations				
CVE-2020-28500	□ Vendor Confirmed				
grunt@0.4.2	□ Used in 250	4.17.21	MEDIUM	6.5	
└─ lodash@0.9.2 ←	locations				
CVE-2018-3721	□ Bug Bounty target				
findup-sync@0.1.3	□ Used in 250	4.17.21	CRITICAL	9.1	
└─ lodash@2.4.2 ←	locations				
CVE-2019-10744	□ Vendor Confirmed				
findup-sync@0.1.3	□ Used in 250	4.17.21	MEDIUM	5.0	
└─ lodash@2.4.2 ←	locations				
CVE-2019-1010266					
captains-log@0.11.11	□ Used in 250	4.17.21	HIGH	7.2	
└─ lodash@2.4.1 ←	locations				
CVE-2021-23337	□ Vendor Confirmed				
captains-log@0.11.11	□ Used in 250	4.17.21	HIGH	7.5	
└─ lodash@2.4.1 ←	locations				
CVE-2018-16487	□ Bug Bounty target				
globule@0.1.0	□ Used in 250	4.17.21	MEDIUM	5.3	
└─ lodash@1.0.2 ←	locations				
CVE-2020-28500	□ Vendor Confirmed				
grunt@0.4.2	□ Used in 10	3.3.5	MEDIUM	5.0	
└─ underscore.stri...	locations				
←					
GHSA-v2p6-4mp7-...					
argparse@0.1.16	□ Used in 8	1.12.1	CRITICAL	9.8	
└─ underscore@1.7.0	locations				
← CVE-2021-23358	□ Vendor Confirmed				
geojsonhint@1.1.0	□ Used in 8	1.2.6	CRITICAL	9.8	
└─ minimist@1.1.1 ←	locations				
CVE-2021-44906					

request@2.40.0	Used in 7 locations	6.2.4	HIGH	7.5
qs@1.0.2 ↵				
CVE-2017-1000048	Vendor Confirmed			
socket.io-adapter@0...	Used in 7 locations	3.3.4	HIGH	7.5
socket.io-parse... ↵				
CVE-2020-36049				
captains-log@0.11.11	Used in 250 locations	4.17.21	MEDIUM	5.3
lodash@2.4.1 ↵				
CVE-2020-28500	Vendor Confirmed			
include-all@0.1.6	Used in 10 locations	3.3.5	MEDIUM	5.0
underscore.stri... ↵				
GHSA-v2p6-4mp7-...				
grunt-contrib-cssmi...	Used in 24 locations	4.1.11	LOW	2.0
clean-css@2.1.8 ↵				
GHSA-wxhq-pm8v-...				
anchor@0.10.5	Used in 4 locations	13.7.0	MEDIUM	5.3
validator@3.41.2 ↵				
CVE-2021-3765	Bug Bounty target			
anchor@0.10.5	Used in 250 locations	4.17.21	HIGH	7.2
lodash@3.9.3 ↵				
CVE-2021-23337	Vendor Confirmed			
engine.io-client@1....	Used in 2 locations	1.1.5	HIGH	7.5
ws@1.0.1 ↵				
GHSA-5v72-xg48-...				
anchor@0.10.5	Used in 250 locations	4.17.21	CRITICAL	9.1
lodash@3.9.3 ↵				
CVE-2019-10744	Vendor Confirmed			
waterline-criteria@...	Used in 250 locations	4.17.21	CRITICAL	9.1
lodash@3.10.1 ↵				
CVE-2019-10744	Vendor Confirmed			
connect@2.30.0	Used in 7 locations	6.2.4	HIGH	7.5
qs@2.4.2 ↵				
CVE-2022-24999	Vendor Confirmed			
grunt@0.4.2	Used in 1 locations	3.13.1	MEDIUM	5.9
js-yaml@2.0.5 ↵				
GHSA-2pr6-76vf-...				
body-parser@1.13.3	Used in 46 locations	2.6.9	HIGH	7.5
debug@2.2.0 ↵				
CVE-2017-20165				
grunt@0.4.2	Used in 250 locations	4.17.21	HIGH	7.5
lodash@0.9.2 ↵				
CVE-2018-16487	Bug Bounty target			
waterline-criteria@...	Used in 250 locations	4.17.21	HIGH	7.2
lodash@3.10.1 ↵				
CVE-2021-23337	Vendor Confirmed			
accepts@1.2.13	Used in 3 locations	0.6.1	HIGH	7.5
negotiator@0.5.3 ↵				
CVE-2016-10539				
anchor@0.10.5	Used in 250 locations	4.17.21	HIGH	7.4
lodash@3.9.3 ↵				
CVE-2020-8203	Bug Bounty target			
engine.io@1.6.11	Used in 2 locations	1.1.5	HIGH	7.5
ws@1.1.0 ↵				
CVE-2016-10542				
form-data@0.1.4	Used in 30 locations	1.4.1	HIGH	7.5
mime@1.2.11 ↵				
CVE-2017-16138				
waterline-criteria@...	Used in 250 locations	4.17.21	HIGH	7.4
lodash@3.10.1 ↵				
CVE-2020-8203	Bug Bounty target			
engine.io@1.6.11	Used in 2 locations	1.1.5	HIGH	7.5
ws@1.1.0 ↵				
GHSA-5v72-xg48-...				
glob@3.1.21	Used in 14 locations	3.0.5	HIGH	7.5
minimatch@0.2.14 ↵				
CVE-2016-10540				
glob@3.1.21	Used in 14 locations	3.0.5	HIGH	7.5
minimatch@0.2.14 ↵				
CVE-2022-3517	Vendor Confirmed			
sails-generate-cont...	Used in 10 locations	3.3.5	MEDIUM	5.0
underscore.stri... ↵				
GHSA-v2p6-4mp7-...				
grunt@0.4.2	Used in 250 locations	4.17.21	HIGH	7.2
lodash@0.9.2 ↵				
CVE-2021-23337	Vendor Confirmed			
rc@0.5.5	Used in 8 locations	0.2.4	CRITICAL	9.8
minimist@0.0.10 ↵				
CVE-2021-44906				
socket.io-adapter@0...	Used in 7 locations	3.3.4	HIGH	7.3
socket.io-parse... ↵				
CVE-2023-32695				
serve-static@1.10.3	Used in 2 locations	0.19.0	MEDIUM	5.0

└─ send@0.13.2 ← CVE-2024-43799	locations						
request@2.40.0	▣ Indirect	0.6.0	MEDIUM	5.0			
└─ tunnel-agent@0.... ← GHSA-xc7v-wxcw-...	dependency						
debug@2.2.0	▣ Used in 7	2.0.0	MEDIUM	5.3			
└─ ms@0.7.1 ← CVE-2017-20162	locations						
waterline-criteria@...	▣ Used in 250	4.17.21	MEDIUM	5.3			
└─ lodash@3.10.1 ← CVE-2020-28500	locations						
	▣ Vendor Confirmed						
geojsonhint@1.1.0	▣ Used in 8	1.2.6	MEDIUM	5.6			
└─ minimist@1.1.1 ← CVE-2020-7598	locations						
	▣ Vendor Confirmed						
connect@2.30.0	▣ Used in 7	6.2.4	HIGH	7.5			
└─ qs@2.4.2 ← CVE-2017-1000048	locations						
	▣ Vendor Confirmed						
waterline-criteria@...	▣ Used in 250	4.17.21	HIGH	7.5			
└─ lodash@3.10.1 ← CVE-2018-16487	locations						
	▣ Bug Bounty target						
anchor@0.10.5	▣ Used in 250	4.17.21	HIGH	7.5			
└─ lodash@3.9.3 ← CVE-2018-16487	locations						
	▣ Bug Bounty target						
grunt@0.4.2	▣ Used in 250	4.17.21	CRITICAL	9.1			
└─ lodash@0.9.2 ← CVE-2019-10744	locations						
	▣ Vendor Confirmed						
grunt@0.4.2	▣ Used in 250	4.17.21	MEDIUM	5.3			
└─ lodash@0.9.2 ← CVE-2020-28500	locations						
	▣ Vendor Confirmed						
globule@0.1.0	▣ Used in 250	4.17.21	HIGH	7.5			
└─ lodash@1.0.2 ← CVE-2018-16487	locations						
	▣ Bug Bounty target						
findup-sync@0.1.3	▣ Used in 14	3.0.5	HIGH	7.5			
└─ minimatch@0.3.0 ← CVE-2016-10540	locations						
grunt@0.4.2	▣ Used in 1	3.13.1	HIGH	7.5			
└─ js-yaml@2.0.5 ← GHSA-8j8c-7jfh-...	locations						
anchor@0.10.5	▣ Used in 250	4.17.21	MEDIUM	5.0			
└─ lodash@3.9.3 ← CVE-2019-1010266	locations						
captains-log@0.11.11	▣ Used in 250	4.17.21	MEDIUM	5.0			
└─ lodash@2.4.1 ← CVE-2019-1010266	locations						
tiny-lr@0.0.4	▣ Used in 46	2.6.9	HIGH	7.5			
└─ debug@0.7.4 ← CVE-2017-20165	locations						
globule@0.1.0	▣ Used in 250	4.17.21	CRITICAL	9.1			
└─ lodash@1.0.2 ← CVE-2019-10744	locations						
	▣ Vendor Confirmed						

Next Steps

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

Top Priority (JS)							
Package	CVEs	Fix Version	Reachable				
uid-safe@2.0.0	GHSA-j4mr-9xw3-c9jx	2.0.0					
└─ base64-url@1.2.1 ← GHSA-j4mr-9xw3-c9jx							
findup-sync@0.1.3	CVE-2018-16487	4.17.21					
└─ lodash@2.4.2 ← CVE-2018-16487							
captains-log@0.11.11	CVE-2018-16487	4.17.21					
└─ lodash@2.4.1 ← CVE-2018-16487							
grunt@0.4.2	CVE-2018-16487	4.17.21					
└─ lodash@0.9.2 ← CVE-2018-16487							
anchor@0.10.5	CVE-2020-8203	4.17.21					
└─ lodash@3.9.3 ← CVE-2020-8203	CVE-2018-16487						
waterline-criteria@1.0.1	CVE-2020-8203	4.17.21					
└─ lodash@3.10.1 ← CVE-2020-8203	CVE-2018-16487						
globule@0.1.0	CVE-2018-16487	4.17.21					
└─ lodash@1.0.2 ← CVE-2018-16487							

Recommendation

▣ 89 out of 153 vulnerabilities requires your attention.

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