

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-hook-grunt@3.... └─ lodash@4.17.5 ← CVE-2019-1010266	Used in 798 locations	4.17.21	MEDIUM	5.0
grunt-legacy-util@1... └─ underscore.string@4.3.0 ← NPM-1085693	Used in 3 locations	3.3.5	MEDIUM	5.0
sails-hook-grunt@3.... └─ eslint@4.11.0 └─ js-yaml@3.13.1 ← NPM-1085724	Used in 10 locations	3.13.1	MEDIUM	5.9
sails-hook-grunt@3.... └─ websocket-extensions@0.1.3 ← CVE-2020-7662	Used in 1 locations	0.1.4	HIGH	8.2
tiny-lr@0.2.1 └─ qs@5.1.0 ← CVE-2017-1000048	Used in 10 locations	6.2.4	HIGH	7.5
sails-hook-grunt@3.... └─ extend@3.0.1 ← CVE-2018-16492	Used in 12 locations	3.0.2	MEDIUM	5.0
sails-hook-grunt@3.... └─ growl@1.9.2 ← CVE-2017-16042	Used in 2 locations	1.10.0	CRITICAL	9.8
connect-redis@3.2.0 └─ redis@2.8.0 ← CVE-2021-29469	Used in 7 locations	3.1.1	HIGH	7.5
sails-hook-grunt@3.... └─ sshpk@1.13.1 ← CVE-2018-3737	Used in 6 locations	1.13.2	HIGH	7.5
socket.io@2.0.3 └─ engine.io@3.1.5 ← CVE-2020-36048	Used in 1 locations	3.6.1	HIGH	7.5
socket.io@2.0.3 └─ engine.io@3.1.5 ← CVE-2022-41940	Used in 1 locations	3.6.1	MEDIUM	6.5
socket.io-client@2.... └─ socket.io-parser@3.1.3 ← CVE-2020-36049	Used in 7 locations	3.3.4	HIGH	7.5
sails-hook-grunt@3.... └─ hosted-git-info@2.8.9 ← CVE-2021-23362	Used in 2 locations	2.8.9	MEDIUM	5.3
sails-hook-grunt@3.... └─ grunt@1.0.1 ← CVE-2020-7729	Indirect dependency	1.5.3	HIGH	7.1
pac-resolver@3.0.0 └─ netmask@1.0.6 ← CVE-2021-28918	Used in 1 locations	1.1.0	CRITICAL	9.1
sails-hook-grunt@3.... └─ stringstream@0.0.6 ← CVE-2018-21270	Used in 4 locations	0.0.6	MEDIUM	5.0
pac-proxy-agent@2.0... └─ pac-resolver@3.0.0 ← CVE-2021-23406	Used in 1 locations	5.0.0	HIGH	8.1
pac-resolver@3.0.0 └─ degenerator@1.0.11 ← CVE-2021-23406	Used in 1 locations	3.0.1	HIGH	8.1
sails-hook-grunt@3.... └─ grunt@1.0.1 ← CVE-2022-1537	Indirect dependency	1.5.3	HIGH	7.0
sails-hook-grunt@3.... └─ grunt@1.0.1 ← CVE-2022-0436	Indirect dependency	1.5.3	MEDIUM	5.5
sails-hook-grunt@3.... └─ clean-css@3.4.28 ← NPM-1091669	Used in 1 locations	4.1.11	LOW	2.0
sails-disk@1.1.2 └─ nedb@1.8.0 ← CVE-2021-23395	Used in 1 locations		HIGH	7.3
grunt-legacy-util@1... └─ getobject@0.1.0 ← CVE-2020-28282	Used in 2 locations	1.0.0	CRITICAL	9.8
pac-resolver@3.0.0 └─ netmask@1.0.6 ← CVE-2021-29418	Used in 1 locations	2.0.1	MEDIUM	5.3
sails-hook-sockets@... └─ socket.io@2.0.3 ← CVE-2020-28481	Used in 1 locations	2.5.1	MEDIUM	4.3
jquery@3.2.1 ← CVE-2020-11022	Used in 2 locations	3.5.0	MEDIUM	6.9

body-parser@1.14.2 └─ ms@0.7.1 ← CVE-2017-20162	Used in 22 locations	2.0.0	MEDIUM	5.3
body-parser@1.14.2 └─ debug@2.2.0 ← CVE-2017-20165	Used in 107 locations	2.6.9	HIGH	7.5
sails-hook-grunt@3.... └─ lodash@4.17.5 ← CVE-2018-16487	Used in 798 locations	4.17.21	HIGH	7.5
sails-hook-grunt@3.... └─ lodash@4.17.5 ← CVE-2020-28500	Used in 798 locations	4.17.21	MEDIUM	5.3
sails-hook-grunt@3.... └─ diff@1.4.0 ← NPM-1095029	Used in 2 locations	3.5.0	HIGH	7.5
sails-hook-grunt@3.... └─ cryptiles@3.1.2 ← CVE-2018-1000620	Used in 4 locations	4.1.2	CRITICAL	9.8
sails-hook-grunt@3.... └─ json-schema@0.2... ← CVE-2021-3918	Used in 2 locations	0.4.0	CRITICAL	9.8
sails-hook-grunt@3.... └─ eslint@4.11.0 └─ js-yaml@3.1... ← NPM-1095058	Used in 10 locations	3.13.1	HIGH	7.5
request@2.85.0 └─ hawk@6.0.2 ← CVE-2022-29167	Used in 2 locations	9.0.1	HIGH	7.4
engine.io-client@3.... └─ xmlhttprequest-... ← CVE-2020-28502	Used in 3 locations	1.6.2	CRITICAL	9.8
engine.io-client@3.... └─ xmlhttprequest-... ← CVE-2021-31597	Used in 3 locations	1.6.2	CRITICAL	9.4
binary-search-tree@... └─ underscore@1.4.4 ← CVE-2021-23358	Used in 11 locations	1.12.1	CRITICAL	9.8
meow@3.7.0 └─ trim-newlines@1... ← CVE-2021-33623	Used in 2 locations	3.0.1	HIGH	7.5
sails-hook-grunt@3.... └─ lodash@4.17.5 ← CVE-2020-8203	Used in 798 locations	4.17.21	HIGH	7.4
sails-hook-grunt@3.... └─ hoek@4.2.1 ← CVE-2020-36604	Used in 10 locations		HIGH	8.1
mkdirp@0.5.1 └─ minimist@0.0.8 ← CVE-2020-7598	Used in 8 locations	0.2.4	MEDIUM	5.6
tiny-lr@0.2.1 └─ qs@5.1.0 ← CVE-2022-24999	Used in 10 locations	6.2.4	HIGH	7.5
sails-hook-grunt@3.... └─ minimatch@3.0.4 ← CVE-2022-3517	Used in 34 locations	3.0.5	HIGH	7.5
sails-hook-grunt@3.... └─ json5@0.5.1 ← CVE-2022-46175	Used in 1 locations	1.0.2	HIGH	7.1
sails-hook-grunt@3.... └─ request@2.83.0 ← CVE-2023-28155	Used in 4 locations		MEDIUM	6.1
body-parser@1.14.2 └─ debug@2.2.0 ← CVE-2017-16137	Used in 107 locations	2.6.9	LOW	3.7
sails-hook-grunt@3.... └─ babel-traverse@... ← CVE-2023-45133	Used in 8 locations		CRITICAL	9.4
sails-hook-grunt@3.... └─ lodash@4.17.5 ← CVE-2021-23337	Used in 798 locations	4.17.21	HIGH	7.2
socket.io-client@2.... └─ socket.io-parse... ← CVE-2022-2421	Used in 7 locations	3.3.4	CRITICAL	9.8
sails-hook-grunt@3.... └─ lodash@4.17.5 ← CVE-2019-10744	Used in 798 locations	4.17.21	CRITICAL	9.1
jquery@3.2.1 ← CVE-2019-11358	Used in 2 locations	3.5.0	MEDIUM	6.1
jquery@3.2.1 ← CVE-2020-11023	Used in 2 locations	3.5.0	MEDIUM	6.9
mkdirp@0.5.1 └─ minimist@0.0.8 ← CVE-2021-44906	Used in 8 locations	0.2.4	CRITICAL	9.8

sails-hook-grunt@3....	Used in 2 locations	4.1.3	MEDIUM	6.5
└─ tough-cookie@2....				
└─ ← CVE-2023-26136				
socket.io-client@2....	Used in 7 locations	3.3.4	HIGH	7.3
└─ socket.io-parse...				
└─ ← CVE-2023-32695				
engine.io@3.1.5	Used in 3 locations	5.2.4	HIGH	7.5
└─ ws@3.3.3 ←				
└─ CVE-2024-37890				
sails-hook-sockets@...	Used in 1 locations	2.5.1	HIGH	7.3
└─ socket.io@2.0.3				
└─ ← CVE-2024-38355				
sails-hook-grunt@3....	Used in 14 locations	5.7.2	HIGH	7.5
└─ semver@5.5.0 ←				
└─ CVE-2022-25883				
socks@1.1.10	Used in 2 locations		HIGH	8.1
└─ ip@1.1.9 ←				
└─ CVE-2024-29415				
sails-hook-grunt@3....	Used in 4 locations	1.20.3	HIGH	7.5
└─ body-parser@1.1...				
└─ ← CVE-2024-45590				
serve-static@1.13.1	Used in 4 locations	0.19.0	MEDIUM	5.0
└─ send@0.16.1 ←				
└─ CVE-2024-43799				
sails@1.5.11	Used in 2 locations	1.16.0	MEDIUM	5.0
└─ serve-static@1....				
└─ ← CVE-2024-43800				
sails@1.5.11	Used in 4 locations	4.20.0	MEDIUM	5.0
└─ express@4.19.2 ←				
└─ CVE-2024-43796				
sails@1.5.11	Used in 4 locations	1.9.0	HIGH	7.5
└─ path-to-regexp@...				
└─ ← CVE-2024-45296				
grunt@1.0.1	Used in 10 locations	3.13.1	MEDIUM	5.9
└─ js-yaml@3.5.5 ←				
└─ GHSA-2pr6-76vf-...				
machinepack-urls@3....	Used in 798 locations	4.17.21	CRITICAL	9.1
└─ lodash@2.4.2 ←				
└─ CVE-2019-10744	Vendor Confirmed			
sails-hook-grunt@3....	Used in 10 locations	3.13.1	HIGH	7.5
└─ eslint@4.11.0				
└─ js-yaml@3.1...				
└─ ←				
└─ GHSA-8j8c-7...				
machinepack-http@6....	Used in 4 locations		MEDIUM	6.1
└─ request@2.85.0 ←				
└─ CVE-2023-28155				
sails-hook-grunt@3....	Used in 1 locations	4.1.11	LOW	2.0
└─ clean-css@3.4.28				
└─ ←				
└─ GHSA-wxhq-pm8v-...				
machinepack-urls@3....	Used in 798 locations	4.17.21	MEDIUM	5.3
└─ lodash@2.4.2 ←				
└─ CVE-2020-28500	Vendor Confirmed			
include-all@1.0.8	Used in 798 locations	4.17.21	MEDIUM	5.3
└─ lodash@3.10.1 ←				
└─ CVE-2020-28500	Vendor Confirmed			
machinepack-urls@3....	Used in 798 locations	4.17.21	HIGH	7.2
└─ lodash@2.4.2 ←				
└─ CVE-2021-23337	Vendor Confirmed			
proxy-agent@2.1.0	Used in 2 locations	2.2.3	CRITICAL	9.1
└─ https-proxy-age...				
└─ ← CVE-2018-3739	Bug Bounty target			
proxy-agent@2.1.0	Used in 2 locations	2.1.0	HIGH	7.5
└─ http-proxy-agen...				
└─ ←	Bug Bounty target			
└─ GHSA-8w57-jfpm-...				
request@2.85.0	Used in 2 locations	4.1.3	MEDIUM	6.5
└─ tough-cookie@2....				
└─ ← CVE-2023-26136	Vendor Confirmed			
include-all@1.0.8	Used in 798 locations	4.17.21	CRITICAL	9.1
└─ lodash@3.10.1 ←				
└─ CVE-2019-10744	Vendor Confirmed			
boom@4.3.1	Used in 10 locations		HIGH	8.1
└─ hoek@4.3.1 ←				
└─ CVE-2020-36604				
include-all@1.0.8	Used in 798 locations	4.17.21	HIGH	7.2
└─ lodash@3.10.1 ←				
└─ CVE-2021-23337	Vendor Confirmed			
body-parser@1.14.2	Used in 10 locations	6.2.4	HIGH	7.5
└─ qs@5.2.0 ←				
└─ CVE-2022-24999	Vendor Confirmed			
grunt-legacy-log-ut...	Used in 798 locations	4.17.21	MEDIUM	5.3
└─ lodash@4.3.0 ←				
└─ CVE-2020-28500	Vendor Confirmed			

har-validator@5.0.3	Used in 6	6.12.3	MEDIUM	5.6
└─ ajv@5.5.2 ←	locations			
CVE-2020-15366	Bug Bounty target			
sails-hook-grunt@3....	Used in 8	1.2.6	CRITICAL	9.8
└─ minimist@1.2.0 ←	locations			
CVE-2021-44906				
machinepack-urls@3....	Used in 798	4.17.21	HIGH	7.5
└─ lodash@2.4.2 ←	locations			
CVE-2018-16487	Bug Bounty target			
sails-hook-grunt@3....	Used in 10	6.5.3	HIGH	7.5
└─ qs@6.5.1 ←	locations			
CVE-2022-24999	Vendor Confirmed			
grunt-legacy-log-ut...	Used in 798	4.17.21	HIGH	7.4
└─ lodash@4.3.0 ←	locations			
CVE-2020-8203	Bug Bounty target			
hawk@6.0.2	Used in 4	4.1.2	CRITICAL	9.8
└─ cryptiles@3.2.1 ←	locations			
CVE-2018-1000620				
grunt-legacy-log-ut...	Used in 798	4.17.21	MEDIUM	5.0
└─ lodash@4.3.0 ←	locations			
CVE-2019-1010266				
include-all@1.0.8	Used in 798	4.17.21	HIGH	7.4
└─ lodash@3.10.1 ←	locations			
CVE-2020-8203	Bug Bounty target			
serve-static@1.15.0	Used in 4	0.19.0	MEDIUM	5.0
└─ send@0.18.0 ←	locations			
CVE-2024-43799				
sails-hook-grunt@3....	Used in 8	1.2.6	MEDIUM	5.6
└─ minimist@1.2.0 ←	locations			
CVE-2020-7598	Vendor Confirmed			
proxy-agent@2.1.0	Used in 2	2.1.0	CRITICAL	9.8
└─ http-proxy-agen...	locations			
← CVE-2019-10196	Vendor Confirmed			
machinepack-urls@3....	Used in 798	4.17.21	MEDIUM	6.5
└─ lodash@2.4.2 ←	locations			
CVE-2018-3721	Bug Bounty target			
grunt-legacy-log-ut...	Used in 798	4.17.21	HIGH	7.5
└─ lodash@4.3.0 ←	locations			
CVE-2018-16487	Bug Bounty target			
inquirer@3.3.0	Used in 12	3.0.1	HIGH	7.5
└─ string-width@2....	locations			
└─ ansi-regex@... ←	Bug Bounty target			
←	Vendor Confirmed			
CVE-2021-38...				
express@4.19.2	Used in 4	1.20.3	HIGH	7.5
└─ body-parser@1.2...	locations			
← CVE-2024-45590				
express@4.19.2	Used in 4	0.1.10	HIGH	7.5
└─ path-to-regexp@...	locations			
← CVE-2024-45296				
grunt-legacy-log-ut...	Used in 798	4.17.21	MEDIUM	6.5
└─ lodash@4.3.0 ←	locations			
CVE-2018-3721	Bug Bounty target			
express@4.19.2	Used in 2	1.16.0	MEDIUM	5.0
└─ serve-static@1....	locations			
← CVE-2024-43800				
grunt@1.0.1	Used in 10	3.13.1	HIGH	7.5
└─ js-yaml@3.5.5 ←	locations			
GHSA-8j8c-7jfh-...				
sails-hook-grunt@3....	Used in 2	3.5.0	HIGH	7.5
└─ diff@1.4.0 ←	locations			
GHSA-h6ch-v84p-...	Vendor Confirmed			
grunt-legacy-log-ut...	Used in 798	4.17.21	HIGH	7.2
└─ lodash@4.3.0 ←	locations			
CVE-2021-23337	Vendor Confirmed			
body-parser@1.14.2	Used in 10	6.2.4	HIGH	7.5
└─ qs@5.2.0 ←	locations			
CVE-2017-1000048	Vendor Confirmed			
include-all@1.0.8	Used in 798	4.17.21	MEDIUM	5.0
└─ lodash@3.10.1 ←	locations			
CVE-2019-1010266				
sails-hook-sockets@...	Used in 7	3.1.1	HIGH	7.5
└─ redis@2.6.3 ←	locations			
CVE-2021-29469				
include-all@1.0.8	Used in 798	4.17.21	MEDIUM	6.5
└─ lodash@3.10.1 ←	locations			
CVE-2018-3721	Bug Bounty target			
proxy-agent@2.1.0	Used in 2	2.2.3	MEDIUM	6.1
└─ https-proxy-age...	locations			
←	Bug Bounty target			
GHSA-pc5p-h8pf-...				
sails-hook-grunt@3....	Used in 10	3.13.1	MEDIUM	5.9
└─ eslint@4.11.0	locations			
└─ js-yaml@3.1...				
←				
GHSA-2pr6-7...				

<div>machinepack-urls@3....</div> <div>└─ lodash@2.4.2 ←</div> <div>CVE-2019-1010266</div>	<div>Used in 798 locations</div> <div>Vendor Confirmed</div>	4.17.21	MEDIUM	5.0
<div>sails-hook-organics...</div> <div>└─ async@2.0.1 ←</div> <div>CVE-2021-43138</div>	<div>Used in 71 locations</div> <div>Vendor Confirmed</div>	2.6.4	HIGH	7.8
<div>mailgun-js@0.13.1</div> <div>└─ async@2.5.0 ←</div> <div>CVE-2021-43138</div>	<div>Used in 71 locations</div> <div>Vendor Confirmed</div>	2.6.4	HIGH	7.8
<div>grunt-legacy-util@1...</div> <div>└─ underscore.stri... ←</div> <div>GHSA-v2p6-4mp7-...</div>	<div>Used in 3 locations</div>	3.3.5	MEDIUM	5.0
<div>grunt-legacy-log-ut...</div> <div>└─ lodash@4.3.0 ←</div> <div>CVE-2019-10744</div>	<div>Used in 798 locations</div> <div>Vendor Confirmed</div>	4.17.21	CRITICAL	9.1
<div>include-all@1.0.8</div> <div>└─ lodash@3.10.1 ←</div> <div>CVE-2018-16487</div>	<div>Used in 798 locations</div> <div>Bug Bounty target</div>	4.17.21	HIGH	7.5

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
<div>proxy-agent@2.1.0</div> <div>└─ https-proxy-agent@1.0.0 ←</div> <div>└─ CVE-2018-3739</div>	CVE-2018-3739	2.2.3	
<div>proxy-agent@2.1.0</div> <div>└─ http-proxy-agent@1.0.0 ←</div> <div>GHSA-8w57-jfpm-945m</div>	GHSA-8w57-jfpm-945m	2.1.0	
<div>machinepack-urls@3.1.1</div> <div>└─ lodash@2.4.2 ←</div> <div>CVE-2018-16487</div>	CVE-2018-16487	4.17.21	
<div>grunt-legacy-log-utils@1.0.0</div> <div>└─ lodash@4.3.0 ←</div> <div>CVE-2020-8203</div>	CVE-2020-8203 CVE-2018-16487	4.17.21	
<div>include-all@1.0.8</div> <div>└─ lodash@3.10.1 ←</div> <div>CVE-2020-8203</div>	CVE-2020-8203 CVE-2018-16487	4.17.21	
<div>inquirer@3.3.0</div> <div>└─ string-width@2.1.1</div> <div>└─ ansi-regex@3.0.0 ←</div> <div>CVE-2021-3807</div>	CVE-2021-3807	3.0.1	

Recommendation	
<div>69 out of 114 vulnerabilities requires your attention.</div> <div>You can remediate 66 vulnerabilities by updating the packages using the fix version</div>	