

Trivy Vulnerability Report

Target: package-lock.json

Package	Version	Vulnerability ID	Severity	Title	Fixed Version
body-parser	1.20.2	CVE-2024-45590	HIGH	body-parser: Denial of Service Vulnerability in body-parser	1.20.3
brace-expansion	1.1.11	CVE-2025-5889	LOW	brace-expansion: juliangruber brace-expansion index.js expand redos	2.0.2, 1.1.12, 3.0.1, 4.0.1
braces	3.0.2	CVE-2024-4068	HIGH	braces: fails to limit the number of characters it can handle	3.0.3
cookie	0.5.0	CVE-2024-47764	LOW	cookie: cookie accepts cookie name, path, and domain with out of bounds characters	0.7.0
express	4.18.3	CVE-2024-29041	MEDIUM	express: cause malformed URLs to be evaluated	4.19.2, 5.0.0-beta.3
express	4.18.3	CVE-2024-43796	LOW	express: Improper Input Handling in Express Redirects	4.20.0, 5.0.0
mongodb	4.1.4	CVE-2021-32050	MEDIUM	Some MongoDB Drivers may erroneously publish events containing authent ...	3.6.10, 4.17.0, 5.8.0
mongoose	8.2.2	CVE-2025-23061	CRITICAL	Mongoose search injection vulnerability	8.9.5, 7.8.4, 6.13.6
mongoose	8.2.2	CVE-2024-53900	HIGH	Mongoose search injection vulnerability	8.8.3, 7.8.3, 6.13.5
path-to-regexp	0.1.7	CVE-2024-45296	HIGH	path-to-regexp: Backtracking regular expressions cause ReDoS	1.9.0, 0.1.10, 8.0.0, 3.3.0, 6.3.0
path-to-regexp	0.1.7	CVE-2024-52798	HIGH	path-to-regexp: path-to-regexp Unpatched `path-to-regexp` ReDoS in 0.1.x	0.1.12
send	0.18.0	CVE-2024-43799	LOW	send: Code Execution Vulnerability in Send Library	0.19.0
serve-static	1.15.0	CVE-2024-43800	LOW	serve-static: Improper Sanitization in serve-static	1.16.0, 2.1.0