



CVE-2021-3918

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2021-3918
State	PUBLIC
Assigner	security@huntr.dev
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-11-13 09:15:00 UTC
Updated	2023-02-03 19:15:00 UTC
Description	json-schema is vulnerable to Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')

Risk And Classification

Problem Types: CWE-1321

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Application	Json-schema Project	Json-schema	All	All	All	All

References

Reference	Source	Link
[SECURITY] [DLA 3228-1] node-json-schema security update	MLIST	lists.debian.
huntr: Prototype Pollution JavaScript Vulnerability in json-schema	CONFIRM	huntr.dev
Don't allow __proto__ property to be used for schema default/coerce, ... · kriszyp/json-schema@22f1461 · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.or
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[159554](#) Oracle Enterprise Linux Security Update for nodejs:16 (ELSA-2021-5171)

[159622](#) Oracle Enterprise Linux Security Update for nodejs:14 (ELSA-2022-0350)

[180175](#) Debian Security Update for node-json-schema (CVE-2021-3918)

181303 Debian Security Update for node-json-schema (DLA 3228-1)
199361 Ubuntu Security Notification for JSON Schema Vulnerability (USN-6103-1)
239970 Red Hat Update for nodejs:16 security (RHSA-2021:5171)
239986 Red Hat Update for rh-nodejs14-nodejs and rh-nodejs14-nodejs-nodemon (RHSA-2022:0041)
240037 Red Hat Update for nodejs:14 security (RHSA-2022:0246)
240051 Red Hat Update for nodejs:14 security (RHSA-2022:0350)
240414 Red Hat Update for rh-nodejs12-nodejs security (RHSA-2022:4914)
377422 Alibaba Cloud Linux Security Update for nodejs:14 (ALINUX3-SA-2022:0014)
377909 Oracle PeopleSoft Enterprise PeopleTools Product Multiple Vulnerabilities (CPUJAN2023)
751759 SUSE Enterprise Linux Security Update for nodejs8 (SUSE-SU-2022:0563-1)
751773 SUSE Enterprise Linux Security Update for nodejs12 (SUSE-SU-2022:0657-1)
751781 OpenSUSE Security Update for nodejs12 (openSUSE-SU-2022:0657-1)
751783 SUSE Enterprise Linux Security Update for nodejs8 (SUSE-SU-2022:0704-1)
751801 SUSE Enterprise Linux Security Update for nodejs14 (SUSE-SU-2022:0715-1)
751820 OpenSUSE Security Update for nodejs14 (openSUSE-SU-2022:0715-1)
751824 OpenSUSE Security Update for nodejs8 (openSUSE-SU-2022:0704-1)
751826 OpenSUSE Security Update for nodejs8 (openSUSE-SU-22022:20000-2)
752142 SUSE Enterprise Linux Security Update for nodejs10 (SUSE-SU-2022:1717-1)
754116 SUSE Enterprise Linux Security Update for SUSE Manager Client Tools (SUSE-SU-2023:2578-1)
755764 SUSE Enterprise Linux Security Update for SUSE Manager Client Tools (SUSE-SU-2024:0487-1)
940355 AlmaLinux Security Update for nodejs:16 (ALSA-2021:5171)
940448 AlmaLinux Security Update for nodejs:14 (ALSA-2022:0350)
960322 Rocky Linux Security Update for nodejs:16 (RLSA-2021:5171)
960863 Rocky Linux Security Update for nodejs:14 (RLSA-2022:0350)
980036 Nodejs (npm) Security Update for json-schema (GHSA-896r-f27r-55mw)

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)