



CVE-2019-10752

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

Summary

CVE	CVE-2019-10752
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-10-17 19:15:00 UTC
Updated	2023-11-07 03:02:00 UTC
Description	Sequelize, all versions prior to version 4.44.3 and 5.15.1, is vulnerable to SQL Injection due to sequelize.json() helper funct

Risk And Classification

Problem Types: CWE-89

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sequelizejs	Sequelize	All	All	All	All
Application	Sequelizejs	Sequelize	All	All	All	All

References

Reference	Source	Link
github.com/sequelize/sequelize/commit/9bd0bc1%2C		github.com
SQL Injection in sequelize Snyk	MISC	snyk.io
github.com/sequelize/sequelize/commit/9bd0bc1,	MISC	github.com
Invalid vulnerability	CONFIRM	snyk.io
fix(sequelize.json.fn): use common path extraction for mysql/mariadb/... · sequelize/sequelize@9bd0bc1 · GitHub	MISC	github.com
Page not found Snyk		snyk.io
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This 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](#).

Free CVE JSON API [cve.report/api](#)

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