



CVE-2020-28470

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

Summary

CVE	CVE-2020-28470
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-14 10:15:00 UTC
Updated	2021-07-21 11:39:00 UTC
Description	This affects the package @scullyio/scully before 1.0.9. The transfer state is serialised with the JSON.stringify() function and

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Scully	Scully	All	All	All	All
Application	Scully	Scully	All	All	All	All

References

Reference	Source	Link
Cross-site Scripting (XSS) in @scullyio/scully Snyk	MISC	snyk.io
(fix) prevent possible XSS by encodeing embedded json by SanderElias · Pull Request #1182 · scullyio/scully · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: Philippe De Ryck

Legacy QID Mappings

[981868](#) Nodejs (npm) Security Update for @scullyio/scully (GHSA-r96p-v3cr-gfv8)

© [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](#)