



CVE-2021-21267

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

Summary

CVE	CVE-2021-21267
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-19 21:15:00 UTC
Updated	2022-06-30 19:08:00 UTC
Description	Schema-Inspector is an open-source tool to sanitize and validate JS objects (npm package schema-inspector). In before ve

Risk And Classification

Problem Types: CWE-20 | CWE-400

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netapp	E-series Performance Analyzer	-	All	All	All
Application	Netapp	Oncommand Insight	-	All	All	All
Application	Schema-inspector Project	Schema-inspector	All	All	All	All

References

Reference	Source	Link
schema-inspector	MISC	www.npmjs.com
CVE-2021-21267 Node.js Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
ReDoS in Schema-Inspector (email validation) · Advisory · schema-inspector/schema-inspector · GitHub	CONFIRM	github.com
GHSL-2020-358-redos-Schema-Inspector.md · GitHub	MISC	gist.github.com
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

[982375](#) Nodejs (npm) Security Update for schema-inspector (GHSA-f38p-c2gq-4pmr)

© [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](#).

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