



CVE-2022-31151

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

Summary

CVE	CVE-2022-31151
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-07-21 04:15:00 UTC
Updated	2022-09-29 15:40:00 UTC
Description	Authorization headers are cleared on cross-origin redirect. However, cookie headers which are sensitive headers and are o

Risk And Classification

Problem Types: CWE-601

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nodejs	Undici	All	All	All	All

References

Reference	Source	Link
Cookies uncleared on cross-host / cross-origin redirect · Advisory · nodejs/undici · GitHub	CONFIRM	github.com
HackerOne	MISC	hackerone.com
`authorization` header is not deleted on redirects to third party origins · Issue #872 · nodejs/undici · GitHub	MISC	github.com
CVE-2022-31151 Node.js Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.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

184582 Debian Security Update for node-undici (CVE-2022-31151)

© [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](#)