



CVE-2022-21704

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

Summary

CVE	CVE-2022-21704
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-01-19 23:15:00 UTC
Updated	2023-02-03 19:16:00 UTC
Description	log4js-node is a port of log4js to node.js. In affected versions default file permissions for log files created by the file, fileSync

Risk And Classification

Problem Types: CWE-276

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	Log4js Project	Log4js	All	All	All	All

References

Reference	S
[SECURITY] [DLA 3229-1] node-log4js security update	M
Changed default file modes from 0o644 to 0o600 for better security by peteriman · Pull Request #87 · log4js-node/streamroller · GitHub	M
Changed default file modes from 0o644 to 0o600 for better security by peteriman · Pull Request #1141 · log4js-node/log4js-node · GitHub	M
log4js-node/CHANGELOG.md at v6.4.0 · log4js-node/log4js-node · GitHub	M
Incorrect Default Permissions in log4js · Advisory · log4js-node/log4js-node · GitHub	C
CVE Program record	C
NVD vulnerability detail	N

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[181038](#) Debian Security Update for node-log4js (CVE-2022-21704)

© [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](#)