



CVE-2021-28374

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

Summary

CVE	CVE-2021-28374
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-15 05:15:00 UTC
Updated	2022-06-28 14:11:00 UTC
Description	The Debian courier-authlib package before 0.71.1-2 for Courier Authentication Library creates a /run/courier/authdaemon di

Risk And Classification

Problem Types: CWE-732

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Canonical	Courier-authlib	All	All	All	All
Application	Debian	Courier-authlib	All	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All

References

Reference	Source
#984810 - courier-authlib: CVE-2021-28374: /run/courier/authdaemon directory with weak permissions - Debian Bug report logs	MISC
[SECURITY] [DLA 2625-1] courier-authlib security update	MLIST
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[178542](#) Debian Security Update for courier-authlib (DLA 2625-1)

[180297](#) Debian Security Update for courier-authlib (CVE-2021-28374)

© [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](#)