



PaperCut NG/MF: Path Traversal in Shared Account Synchronization

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

Summary

CVE	CVE-2026-6418
State	PUBLISHED
Assigner	PaperCut
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-05 07:16:00 UTC
Updated	2026-05-05 07:16:00 UTC

Description An issue was discovered in the Shared Account Synchronization component of PaperCut MF (version 25.0.4). The applicat

Risk And Classification

Primary CVSS: v4.0 4.6 MEDIUM from eb41dac7-0af8-4f84-9f6d-0272772514f4

CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:L/VI:N/VA:N/SC:H/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-36 | CWE-552 | CWE-36 CWE-36 Absolute path traversal | CWE-552 CWE-552 Files or directories accessible to external parties

Version	Source	Type	Score	Severity	Vector
4.0	eb41dac7-0af8-4f84-9f6d-0272772514f4	Secondary	4.6	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:L/VI:N/VA:N
4.0	CNA	CVSS	4.6	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:L/VI:N/VA:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

High

User Interaction

None

Confidentiality

Low

Integrity

None

Availability

None

Sub Conf.

High

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:L/VI:N/VA:N/SC:H/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	PaperCut	PaperCut NG/MF	affected 25.0.11 semver	Not specified

References

Reference	Source	Link
www.papercut.com/kb/Main/papercut-ng-mf-and-papercut-hive-security-bulletin-ma...	eb41dac7-0af8-4f84-9f6d-0272772514f4	www.paper...
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© 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