Multiple cross-site scripting (XSS) vulnerabilities in PaperCut NG/MF

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-4794
State	PUBLISHED
Assigner	PaperCut
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-31 01:16:36 UTC
Updated	2026-04-01 14:24:02 UTC
Description	Multiple cross-site scripting (XSS) vulnerabilities in PaperCut NG/MF before 25.0.10 allow authenticated administrator users

Risk And Classification

Primary CVSS: v4.0 2.1 LOW from eb41dac7-0af8-4f84-9f6d-0272772514f4

CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:P/VC:N/VI:N/VA:N/SC:L/SI:L/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/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000440000 probability, percentile 0.135960000 (date 2026-04-02)

Problem Types: CWE-79 | CWE-79 CWE-79 Improper neutralization of input during web page generation ('cross-site scripting')

Version	Source	Type	Score	Severity	Vector
4.0	eb41dac7-0af8-4f84-9f6d-0272772514f4	Secondary	2.1	LOW	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:P/VC:N/VI:N/VA:N/
4.0	CNA	CVSS	2.1	LOW	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:P/VC:N/VI:N/VA:N/

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

Low

User Interaction

Passive

Passive

Confidentiality

None

Integrity

None

Availability

None

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:P/VC:N/VI:N/VA:N/SC:L/SI:L/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/MSC:X/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 25.0.10 semver	Windows, MacOS, Linux

References

Reference	Source	Link	T
www.papercut.com/kb/Main/papercut-ng-mf-security-bulletin-march-2026	eb41dac7-0af8-4f84-9f6d-0272772514f4	www.papercut.com	
CVE Program record	CVE.ORG	www.cve.org	c
NVD vulnerability detail	NVD	nvd.nist.gov	c

No vendor comments have been submitted for this CVE.

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