PaperCut NG/MF Cross-Site Request Forgery (CSRF) Vulnerability

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2023-2533
State	PUBLIC
Assigner	help@fluidattacks.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-06-20 15:15:00 UTC
Updated	2023-07-06 06:15:00 UTC
Description	A Cross-Site Request Forgery (CSRF) vulnerability has been identified in PaperCut NG/MF, which, under specific condition

Risk And Classification

EPSS: 0.363220000 probability, percentile 0.970930000 (date 2026-04-04)

CISA KEV: Listed on 2025-07-28; due 2025-08-18; ransomware use Unknown

Problem Types: CWE-352

CISA Known Exploited Vulnerability

Vendor	PaperCut
Product	NG/MF
Name	PaperCut NG/MF Cross-Site Request Forgery (CSRF) Vulnerability
Required Action	Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.
Notes	https://www.papercut.com/kb/Main/SecurityBulletinJune2023 ; https://nvd.nist.gov/vuln/detail/CVE-2023-2533

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Papercut	Papercut Mf	22.0.10	All	All	All
Application	Papercut	Papercut Ng	22.0.10	All	All	All

References

Reference	Source	Link
PaperCut MF/NG 22.0.10 (Build 65996 2023-03-27) - Remote code execution via CSRF | Advisories | Fluid Attacks	MISC	fluidattacks

PaperCut: Print management software	MISC	www.pape
PaperCut NG/MF Security Bulletin (June 2023) | PaperCut	MISC	www.pape
CVE Program record	CVE.ORG	www.cve.c
NVD vulnerability detail	NVD	nvd.nist.gc
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.g

No vendor comments have been submitted for this CVE.

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