

CVE-2023-27351

PaperCut NG/MF Improper Authentication Vulnerability

CISA KEV since Apr 20, 2026

Actively exploited

Ransomware use known

This vulnerability allows remote attackers to bypass authentication on affected installations of PaperCut NG 22.0.5 (Build 63914). Authentication is not required to exploit this vulnerability. The specific flaw exists within the SecurityRequestFilter class. The issue results from improper implementation of the authentication algorithm. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-19226.

EVRS 87/100 Immediate priority	CVSS V3.1 7.5 High · NVD	EPSS 0.781 99.58th percentile · FIRST	CISA DEADLINE May 4, 2026 CISA federal deadline · Overdue by 6 months
--	--	---	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☒ Ransomware	Known ransomware campaigns	☐ KEV recency	Added to CISA KEV within the last year
☒ EPSS	0.781 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.5	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch Immediately Patch or fixed version identified

CISA 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.
Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
papercut mf	$\geq 15.0 < 20.1.7$ $\geq 21.0.0 < 21.2.11$ $\geq 22.0.0 < 22.0.9$	20.1.7 · 21.2.11 · 22.0.9	NVD
papercut ng	$\geq 15.0 < 20.1.7$ $\geq 21.0.0 < 21.2.11$ $\geq 22.0.0 < 22.0.9$	20.1.7 · 21.2.11 · 22.0.9	NVD

Sources

Vendor guidance github.com/advisories/GHSA-2c69-r2jh-xjvm
NVD nvd.nist.gov/vuln/detail/CVE-2023-27351

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2023-31127

Additional guidance papercut.com/kb/Main/P0-1216-and-P0-1219
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnable.com/vulnerability-management/cve/CVE-2023-27351

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.