



# PaperCut MF/NG Improper Access Control Vulnerability

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

## Summary

<b>CVE</b>	CVE-2023-27350
<b>State</b>	PUBLIC
<b>Assigner</b>	zdi-disclosures@trendmicro.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-04-20 16:15:00 UTC
<b>Updated</b>	2023-06-07 18:15:00 UTC
<b>Description</b>	This vulnerability allows remote attackers to bypass authentication on affected installations of PaperCut NG 22.0.5 (Build 6:

## Risk And Classification

**EPSS:** 0.942570000 probability, percentile 0.999340000 (date 2026-04-04)

**CISA KEV:** Listed on 2023-04-21; due 2023-05-12; ransomware use Known

**Problem Types:** CWE-284

## CISA Known Exploited Vulnerability

<b>Vendor</b>	PaperCut
<b>Product</b>	MF/NG
<b>Name</b>	PaperCut MF/NG Improper Access Control Vulnerability
<b>Required Action</b>	Apply updates per vendor instructions.
<b>Notes</b>	<a href="https://www.papercut.com/kb/Main/PO-1216-and-PO-1219">https://www.papercut.com/kb/Main/PO-1216-and-PO-1219</a> ; <a href="https://nvd.nist.gov/vuln/detail/CVE-2023-27350">https://nvd.nist.gov/vuln/detail/CVE-2023-27350</a>

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Papercut</a>	<a href="#">Papercut Mf</a>	All	All	All	All
Application	<a href="#">Papercut</a>	<a href="#">Papercut Ng</a>	All	All	All	All

## References

Reference	Source	Link	Tags
PaperCut PaperCutNG Authentication Bypass ≈ Packet Storm	MISC	<a href="https://packetstormsecurity.com">packetstormsecurity.com</a>	
Increased exploitation of PaperCut drawing blood around the Internet	MISC	<a href="https://www.cerberus.com">www.cerberus.com</a>	

increased exploitation of PaperCut drawing blood around the internet – Soproos news	MISC	<a href="https://news.sopros.com">news.sopros.com</a>	
PaperCut NG/MG 22.0.4 Authentication Bypass ≈ Packet Storm	MISC	<a href="https://packetstormsecurity.com">packetstormsecurity.com</a>	
PaperCut NG/MG 22.0.4 Remote Code Execution ≈ Packet Storm	MISC	<a href="https://packetstormsecurity.com">packetstormsecurity.com</a>	
PaperCut MF/NG Authentication Bypass / Remote Code Execution ≈ Packet Storm	MISC	<a href="https://packetstormsecurity.com">packetstormsecurity.com</a>	
ZDI-23-233   Zero Day Initiative	MISC	<a href="https://www.zerodayinitiative.com">www.zerodayinitiative.com</a>	
APRIL 19 UPDATE   PaperCut MF/NG vulnerability bulletin (March 2023)   PaperCut	MISC	<a href="https://www.papercut.com">www.papercut.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical,
CISA Known Exploited Vulnerabilities catalog	CISA	<a href="https://www.cisa.gov">www.cisa.gov</a>	kev

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[150721](#) PaperCut NG/MF Remote Code Execution (RCE) Vulnerability (CVE-2023-27350)

[378441](#) PaperCut NG Remote Code Execution (RCE) Vulnerability

[730790](#) PaperCut NG/MF Multiple Security Vulnerabilities (PO-1216 and PO-1219)

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)**