



PaperCut MF/NG Improper Access Control Vulnerability

Critical vulnerability in PaperCut Print Management Server exploited in the wild

<https://www.papercut.com/kb/Main/PO-1216-and-PO-1219>
 CVEs: [CVE-2023-27350](#)

An unauthenticated attacker can perform a Remote Code Execution (RCE) on a vulnerable PaperCut Application Server. According to the vendor, the specific flaw exists within the SetupCompleted class and could be achieved remotely without authentication. PaperCut MF/NG Improper Access Control Vulnerability (CVE-2023-27350) has been seen exploited in the wild.

Background	Papercut is a company which offers a print management system called PaperCut MF and PaperCut NG, which provides print monitoring and control capabilities supporting a wide range of different printers, scanners, and other devices for that purpose. Successful exploitation of this security defect allows a remote, unauthenticated attacker to bypass authentication and execute arbitrary code with system privileges. According to a Shodan search, there are approximately 1700 internet exposed PaperCut application servers.
Announced	<p>January 10, 2023: Zero Day Initiative disclosed the vulnerabilities to PaperCut. https://www.zerodayinitiative.com/advisories/ZDI-23-233/ https://www.zerodayinitiative.com/advisories/ZDI-23-232/</p> <p>March 8, 2023: PaperCut released a patch and advises to immediately upgrade PaperCut Application Servers to one of the fixed versions provided. https://www.papercut.com/kb/Main/PO-1216-and-PO-1219</p>
Latest Developments	<p>April 19, 2023: Vendor reported that unpatched servers are being exploited in the wild, particularly the flaw CVE-2023-27350.</p> <p>April 24, 2023: CISA added CVE-2023-27350 to its known exploited vulnerabilities catalog (KEV).</p> <p>May 11, 2023: CISA and FBI Release Joint Advisory in Response to Active Exploitation of PaperCut Vulnerability https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-131a</p> <p>Both CVE-2023-27350, CVE-2023-27351 have been fixed in PaperCut MF and PaperCut NG versions 20.1.7, 21.2.11 and 22.0.9 and later. FortiGuard Labs has released an IPS signature to detect and block attacks leveraging (CVE-2023-27350) which has been seen exploited in the wild. According to PaperCut, there is no evidence that CVE-2023-27351 is being used in the wild. However, it is strongly advised to apply patches for both immediately if not already done.</p>

PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

Reconnaissance

Lure

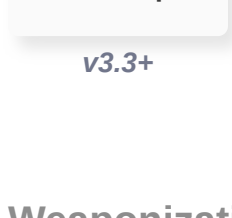
Mitigates PaperCut vulnerability by detecting and preventing lateral movement on the network segment



FortiDeceptor
v3.3+

Decoy VM

Mitigates PaperCut vulnerability by detecting and preventing lateral movement on the network segment



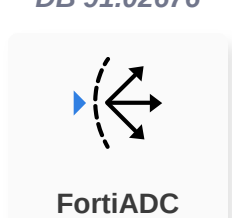
FortiDeceptor
v3.3+

Weaponization

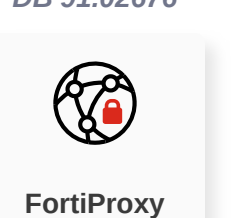
Delivery

AV

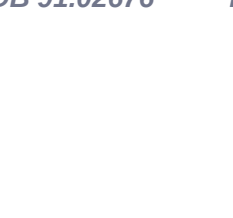
Detects and blocks known malware related to PaperCut MF/NG Improper Access Control Vulnerability (CVE-2023-27350)



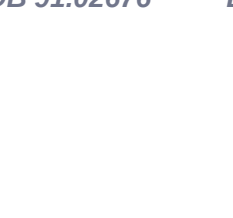
FortiGate
DB 91.02676



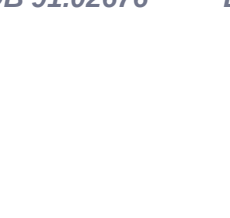
FortiWeb
DB 91.02676



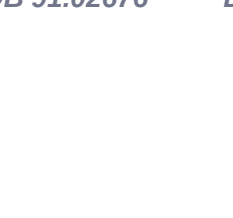
FortiClient
DB 91.02676



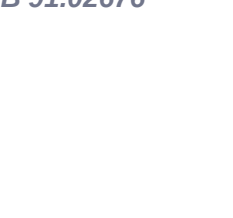
FortiSASE
DB 91.02676



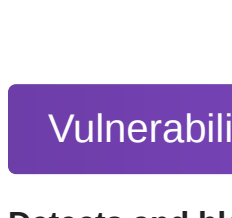
FortiMail
DB 91.02676



FortiCASB
DB 91.02676



FortiCWP
DB 91.02676



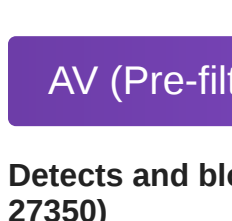
FortiADC
DB 91.02676



FortiProxy
DB 91.02676

Vulnerability

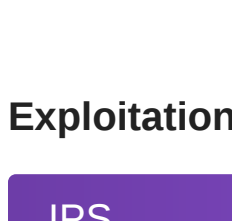
Detects and blocks attack attempts leveraging Papercut MF/NF vulnerability (CVE-2023-27350)



FortiClient
DB 1.445

AV (Pre-filter)

Detects and blocks known malware related to PaperCut MF/NG Improper Access Control Vulnerability (CVE-2023-27350)



FortiEDR
DB 91.02676

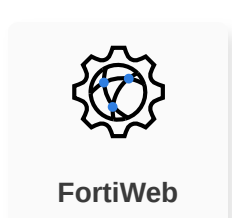


FortiNDR
DB 91.02676

Exploitation

IPS

Detects and blocks attack attempts leveraging Papercut MF/NF vulnerability (CVE-2023-27350)



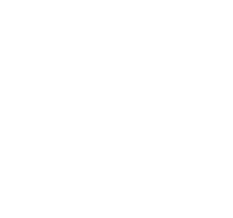
FortiGate
DB 23.541



FortiSASE
DB 23.541



FortiNDR
DB 23.541



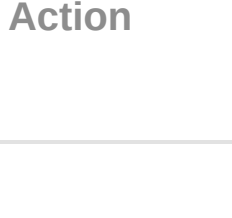
FortiADC
DB 23.541



FortiProxy
DB 23.541

Web App Security

Detects and blocks attack attempts leveraging Papercut MF/NF vulnerability (CVE-2023-27350)



FortiWeb
DB 0.00348

Installation

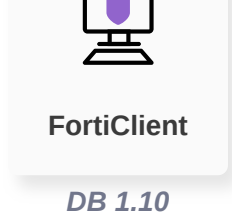
C2

Action

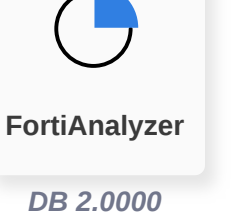
DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

Outbreak Detection

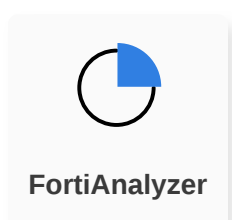


FortiClient
DB 1.10

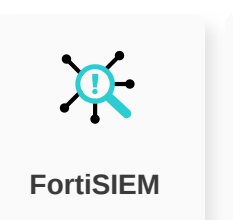


FortiAnalyzer
DB 2.0000

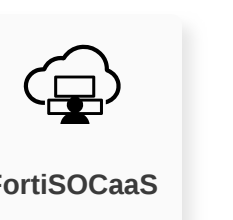
IOC



FortiAnalyzer

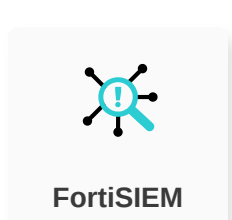


FortiSIEM



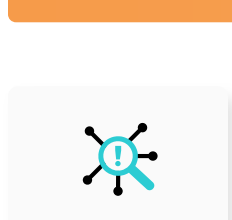
FortiSOCaaS

Content Update



FortiSIEM
DB 315

Threat Hunting



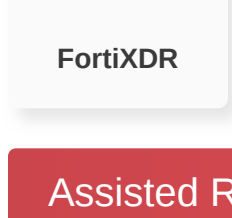
FortiSIEM
v6.6+

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak.



FortiXDR

Assisted Response Services

Experts to assist you with analysis, containment and response activities.



Incident Response



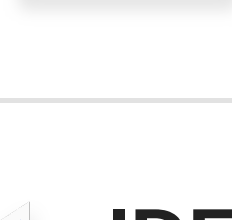
FortiRecon: ACI

RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

InfoSec Services

Security readiness and awareness training for SOC teams, InfoSec and general employees.



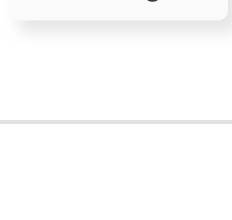
Response Readiness

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Monitoring (Inside & Outside)

Security reconnaissance and penetration testing services, covering both internal & external attack vectors, including those introduced internally via software supply chain.



Security Rating



FortiRecon: EASM

Additional Resources

FortiGuard Threat Signal	https://www.fortiguardsignal.com/threat-signal-report/5147
Bleeping Computer	https://www.bleepingcomputer.com/news/security/exploit-released-for-papercut-flaw-abused-to-hijack-servers-patch-now/
SecurityWeek	https://www.securityweek.com/huntress-most-papercut-installations-not-patched-against-already-exploited-security-flaw/
The Hacker News	https://thehackernews.com/2023/04/russian-hackers-suspected-in-ongoing.html
The Hacker News	https://thehackernews.com/2023/04/microsoft-confirms-papercut-servers.html

Learn more about [FortiGuard Outbreak Alerts](#)

