



CVE-2023-39143

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

Summary

CVE	CVE-2023-39143
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-04 17:15:00 UTC
Updated	2023-08-08 20:07:00 UTC
Description	PaperCut NG and PaperCut MF before 22.1.3 on Windows allow path traversal, enabling attackers to upload, read, or delete files.

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows	-	All	All	All
Application	Papercut	Papercut Mf	All	All	All	All
Application	Papercut	Papercut Ng	All	All	All	All

References

Reference	Source	Link	Tags
CVE-2023-39143: PaperCut Path Traversal/File Upload RCE Vulnerability – Horizon3.ai	MISC	www.horizon3.ai	
PaperCut NG/MF Security Bulletin (July 2023) PaperCut	MISC	www.papercut.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analyzed

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

150719 PaperCut NG/MF Path Traversal Vulnerability (CVE-2023-39143)

378740 PaperCut NG/MF Chained Path Traversal in Authenticated API

700005 PaperCut NG/MF Security Bulletin (July 2023) | PaperCut

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)