UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0338

PAPERCUT BUG EXPOSES SERVERS TO RCE

DATE ISSUED: 9th August 2023

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	**MEDIUM**	EASY

OVERVIEW

A critical vulnerability in PaperCut's NG/MF print management software has been recently disclosed. This vulnerability had the potential to enable unauthorized attackers to execute code remotely on Windows servers that had not been updated.

BREAKDOWN

PaperCut NG and PaperCut MF are print management software solutions designed to help organizations manage and control their printing resources. A critical flaw tracked as CVE-2023-39143 is disclosed in its software which arises from a chain of two path traversal weaknesses discovered by Horizon3 security researchers. It could allow an unauthorised attacker to read, delete, and upload arbitrary files on compromised systems. However, the vulnerability primarily affects non-default server setups where the external device integration option is activated. But according to a report by Horizon3, this setting is commonly enabled on the majority of Windows PaperCut servers. Earlier this year, multiple ransomware groups targeted PaperCut servers by exploiting a separate critical unauthenticated remote code execution vulnerability (CVE-2023–27350) and a significant high-severity information disclosure flaw (CVE-2023–27351).

REMEDIATION STEPS

- Apply security updates and patches provided by PaperCut to address critical vulnerabilities.
- Administrators who are unable to promptly apply security updates can implement an IP address allowlist to restrict access to PaperCut servers. Only permit connections from trusted IP addresses that require access.
- Disable non-essential features or settings, such as external device integration, to reduce the potential attack surface.
- Employ robust monitoring and intrusion detection systems to promptly identify and respond to any suspicious or unauthorised activities.

REFERENCES & RESOURCES

Bleeping Computer https://www.bleepingcomputer.com/news/security/new-papercut-critical-bug-exposes-unpatched-servers-to-rce-attacks/