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

CYBER GUIDANCE ISSUE 0317

RANSOMWARE GROUPS TARGET SCHOOLS VIA PAPERCUT FLAW

DATE ISSUED: 15th May 2023

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

OVERVIEW

In a recent joint Cybersecurity Advisory (CSA) from the FBI and CISA, the Bl00dy Ransomware group is leveraging the PaperCut NG and PaperCut MF remote code execution (RCE) vulnerability to infiltrate networks. It could allow an unauthenticated actor to execute malicious code remotely without credentials.

BREAKDOWN

The Bl00dy ransomware gang targets schools via a critical remote code execution flaw in unpatched PaperCut MF and NG print management software. The PaperCut vulnerability, tracked as CVE-2023-27350 with a CVSS score of 9.8, was patched in March. However, unpatched servers actively face widespread exploitation by various ransomware groups. It could allow malicious actors to bypass user authentication and access the server as an administrator. After accessing the server, actors can leverage existing PaperCut software features for remote code execution (RCE). According to the security advisory, the threat actors focus their attacks on the education sector, which has a significant public exposure of the flaw. According to CISA, the Education Facilities subsector accounts for about 68% of the internet-exposed PaperCut servers. The availability of proof-of-concept (PoC) exploits for the PaperCut flaws, some of which are less detected, raises the risk for organisations even more.

REMEDIATION STEPS

- Upgrade to the latest PaperCut MF and NG versions 20.1.7, 21.2.11, and 22.0.9 and later, which addresses all security gaps exploited by the threat actors.
- If unable to immediately patch, ensure vulnerable PaperCut servers are not accessible over the internet.
- Implement phishing-resistant multifactor authentication (MFA) for all staff and all services.
- Use network traffic monitoring tools to identify unusual traffic and behaviour patterns that may indicate malware activity.
- Check out Unisphere's Ransomware Defence Strategy FREE resource on our website.

REFERENCES & RESOURCES

TechTarget	https://www.techtarget.com/searchsecurity/news/366537554/Bl00dy-ransomware-gang-targets-schools-via-PaperCut-flaw
CISA	https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-131a
Bleeping Computer	https://www.bleepingcomputer.com/news/security/fbi-bl00dy-ransomware-targets-education-orgs-in-papercut-attacks/
SecurityWeek	https://www.securityweek.com/cisa-fbi-ransomware-gang-exploited-papercut-flaw-against-education-facilities/