Hive Pro

Threat Level

Red

CISA: AA23-131A

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Bl00dy Ransomware Exploiting Critical Vulnerability in PaperCut Software

Date of Publication	Last Updated Date	Admiralty Code	TA Number
April 25, 2023	May 15, 2023	A1	TA2023197

Summary

First Seen: January 10, 2023
Affected Products: PaperCut MF and PaperCut NG
Malware: Bl00dy Ransomware, Clop Ransomware, LockBit Ransomware, DiceLoader, TrueBot, and Cobalt Strike Beacons
Impact: The vulnerabilities allow for unauthenticated remote code execution and authentication bypass.

⚙ CVEs

CVE	NAME	AFFECTED PRODUCTS	ZERO DAY	CISA	PATCH
CVE-2023-27350	PaperCut MF/NG Improper Access Control Vulnerability	PaperCut MF and NG	✗	✓	✓
CVE-2023-27351	PaperCut MF/NG Improper Authentication Vulnerability	PaperCut MF and NG	✗	✗	✓

Vulnerability Details

#1

Attackers are exploiting severe vulnerabilities (CVE-2023-27350 and CVE-2023-27351) in PaperCut MF/NG print management software to install Atera remote management software and potentially take over servers. PaperCut printing management software used by roughly 70,000 organizations in over 100 countries. The vulnerabilities allow remote attackers to bypass authentication and execute arbitrary code with SYSTEM privileges. Patches have been released, but proof-of-concept exploits are available online, increasing the risk of further attacks.

#2

The attacks have primarily targeted the education sector, which has a high number of internet-exposed PaperCut servers. The Bl00dy Ransomware gang gained access to victim networks, leading to data exfiltration and encryption of systems, targeting the Education sector. Even the Clop, LockBit ransomware, and the Iranian hacking groups, including 'Muddywater,' have joined in exploiting the vulnerability. The FBI discovered evidence of C2 malware downloads, including DiceLoader, TrueBot, and Cobalt Strike Beacons, but it's unclear when these tools were used in the attack.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-27350	PaperCut MF: before 22.0.9 PaperCut NG: before 22.0.9	cpe:2.3:a:papercut:papercut_ng:*:*:*:*:*:*:*:*	CWE-284
CVE-2023-27351			CWE-287

Recommendations

Promptly update PaperCut servers to the latest patched versions (20.1.7, 21.2.11, or 22.0.9) to mitigate the risk of exploitation.

Implement network access controls, consider blocking traffic to the web management port from external IP addresses to prevent remote exploitation. Block the indicators of compromise (IOCs) related to these vulnerabilities.

Follow security best practices, such as using strong passwords, enabling 2FA, keeping software and systems updated, and restricting access to necessary users. Regularly monitor for malicious activities and educate users about security risks.

Organizations, especially those in the education sector, should closely monitor network activity for signs of exploitation. Pay attention to any unusual network traffic, such as unexpected connections or data transfers. Additionally, monitor child processes, such as the spawning of "cmd.exe" and "powershell.exe," which can indicate malicious activity.

Potential MITRE ATT&CK TTPs

TA0005 Defense Evasion	TA0004 Privilege Escalation	TA0002 Execution	TA0040 Impact
TA0003 Persistence	T1068 Exploitation for Privilege Escalation	T1102 Web Service	T1059 Command and Scripting Interpreter
T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1588.005 Exploits	T1027 Obfuscated Files or Information
T1203 Exploitation for Client Execution	T1562 Impair Defenses	T1056 Input Capture	T1105 Ingress Tool Transfe
T1584 Compromise Infrastructure	T1090 Proxy	T1059.001 PowerShell	T1486 Data Encrypted for Impact

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	46fe07c07fd0f45ba45240ef9aae2a44
SHA1	b918f97c7c6ebc9594de3c8f2d9d75ecc292d02b
SHA256	c0f8aeeb2d11c6e751ee87c40ee609aceb1c1036706a5af0d3d78738b6cc4125 00ec44df6487faf9949cebee179bafe8377ca44177367669325 08f94da0f35fe 6bb160ebdc59395882ff322e67e000a22a5c54ac777b6b1f10f1fef381df9c15 0ce7c6369c024d497851a482e011ef1528ad270e83995d52213276edbe71403f
URLs	hxxp://upd488.windowservicecemter[.]com/download/AppPrint.msi hxxp://upd488.windowservicecemter[.]com/download/setup.msi hxxp://upd488.windowservicecemter[.]com/download/a3.msi
Emails	decrypt.support@privyonline[.]com fimaribahundqf@gmx[.]com main-office@data-highstream[.]com prepalkeinuc0u@gmx[.]com tpyrcne@onionmail[.]org

TYPE	VALUE
Tax ID	E3213A199CDA7618AC22486EFECBD9F8E049AC36094D56AC1BFBE67EB9C3CF2352CAE9EBD35F
Domains	upd343.winserverupdates[.]com upd488.windowservicecemter[.]com anydeskupdate[.]com anydeskupdates[.]com netviewremote[.]com updateservicecenter[.]com windowcsupdates[.]com windowservicecemter[.]com windowservicecentar[.]com windowservicecenter[.]com winserverupdates[.]com ber6vjyb[.]com study.abroad[.]ge upd488.windowservicecemter[.]com/download/update.dll
IPV4	172.67.156[.]5 104.21.73[.]3 102.130.112[.]157 172.106.112[.]46 176.97.76[.]163 192.160.102[.]164 194.87.82[.]7 195.123.246[.]20 198.50.191[.]95 206.197.244[.]75 216.122.175[.]114 46.4.20[.]30 5.188.206[.]14 5.8.18[.]233 5.8.18[.]240 80.94.95[.]103 89.105.216[.]106 92.118.36[.]199 192.184.35[.]216

Patch Links

https://www.papercut.com/kb/Main/PO-1216-and-PO-1219

References

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-131a

https://www.huntress.com/blog/critical-vulnerabilities-in-papercut-print-management-software

https://www.bleepingcomputer.com/news/security/exploit-released-for-papercut-flaw-abused-to-hijack-servers-patch-now/

https://www.cisa.gov/known-exploited-vulnerabilities-catalog

https://arcticwolf.com/resources/blog/cve-2023-27350/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.

Contextualize
Uni5 Threat Exposure Management
Prioritize
Resolve

REPORT GENERATED ON

April 25, 2023 • 03:30 AM

More at www.hivepro.com