URGENT MF/NG vulnerability bulletin (March 2023) | PaperCut

THE PAGE APPLIES TO:

PaperCut NG PaperCut MF PaperCut Pocket PaperCut Hive

Contents

info

This page will continue to be updated as new information becomes available. Last updated: 16 May 12:00 AEST.

We have received two vulnerability reports from a 3rd party cyber security company (Trend Micro), for high/critical severity security issues in PaperCut MF/NG. **We have evidence to suggest that unpatched servers are being exploited in the wild.**

- Remote Code Execution vulnerability (CVE-2023–27350 / ZDI-CAN-18987 / ZDI-23–233)
- User account data vulnerability (CVE-2023–27351 / ZDI-CAN-19226 / ZDI-23–232)

Critical

Please note that as of 18th April, 2023 (see “When was the exploit first detected in the wild?” in the FAQs) we have evidence to suggest that unpatched servers are being exploited in the wild, (particularly ZDI-CAN-18987 / PO-1216 / ZDI-23–233).

Our immediate advice is to upgrade your PaperCut Application Servers to one of the fixed versions listed below if you haven’t already.

If you suspect that your server has been compromised, we recommend taking server backups, then wiping the Application Server, and rebuilding the Application Server and restoring the database from a ‘safe’ backup point prior to when you discovered any suspicious behavior. We have also updated the FAQ “How do I know if my server has been exploited?” question below.

Important

Both of these vulnerabilities have been **fixed** in PaperCut MF and PaperCut NG versions **20.1.7, 21.2.11, and 22.0.9 and later**. We highly recommend upgrading to one of these versions containing the fix (see the Where can I get the upgrade? question below).

ZDI-CAN-18987 / PO-1216 / ZDI-23–233

(also identified as CVE-2023–27350)

ZDI-CAN-19226 / PO-1219 / ZDI-23-232

(also identified as CVE-2023-27351)

We have confirmed that under certain circumstances this allows for an unauthenticated attacker to potentially pull information about a user stored within PaperCut MF or NG - including usernames, full names, email addresses, office/department info and any card numbers associated with the user. The attacker can also retrieve the hashed passwords for **internal** PaperCut-created users only (note that this does **not** include any password hashes for users sync'd from directory sources such as Microsoft 365 / Google Workspace / Active Directory and others). This could be done remotely and without the need to log in. We do not have any evidence of this vulnerability being used against customers at this point.

This vulnerability has been rated with a CVSS score of 8.2.

Product status and next steps

Which PaperCut products are impacted, and what are the actions required?

	ZDI-CAN-18987 / PO-1216 / ZDI-23-233 *CVE-2023-27350*	**ZDI-CAN-19226 / PO-1219 / ZDI-23-232** *CVE-2023-27351*
What versions *are* impacted / which versions are VULNERABLE?	PaperCut MF or NG version 8.0 or later (excluding patched versions) on all OS platforms. This includes: version 8.0.0 to 19.2.7 (inclusive) version 20.0.0 to 20.1.6 (inclusive)	PaperCut MF or NG version 15.0 or later (excluding patched versions), on all OS platforms. This includes: version 15.0.0 to 19.2.7 (inclusive) version 20.0.0 to 20.1.6 (inclusive)

versions are FIXED?	versions 22.0.9 and later	versions 22.0.9 and later
Which PaperCut MF or NG components are impacted?	Application Servers **are** impacted Site Servers **are** impacted	Application Servers **are** impacted
Which PaperCut components or products are *NOT* impacted?	PaperCut MF/NG secondary servers (Print Providers). PaperCut MF/NG Direct Print Monitors (Print Providers). PaperCut MF MFD Embedded Software. PaperCut Hive. PaperCut Pocket. Print Deploy. Mobility Print. PaperCut User Client software. PaperCut Multiverse. Print Logger.	PaperCut MF/NG secondary servers (Print Providers). PaperCut MF/NG Direct Print Monitors (Print Providers). PaperCut MF/NG site servers. PaperCut MF MFD Embedded Software. PaperCut Hive. PaperCut Pocket. Print Deploy. Mobility Print. PaperCut User Client software. PaperCut Multiverse. Print Logger.
Next steps	We recommend that you upgrade all Application Servers and Site Servers (see Upgrade documentation) You will **not** need to patch Secondary Servers (Print Providers / Direct Print Monitors) - but you can if you prefer.	We recommend that you upgrade all Application Servers and Site Servers (see Upgrade documentation). Even though the Site Server is not impacted by this vulnerability, you will need to upgrade them to match the version number of the Application Server. You will **not** need to patch Secondary Servers (Print Providers / Direct Print Monitors) - but you can if you prefer.

Please follow your usual upgrade procedure. Additional links on the 'Check for updates' page (accessed through the Admin interface > About > Version info > Check for updates) will allow customers to download fixes for previous major versions which are still supported (e.g. 20.1.7 and 21.2.11) as well as the current version available.

If you are using PaperCut MF, we highly recommend following your regular upgrade process. Your PaperCut partner or reseller information can also be found on the 'About' tab in the PaperCut admin interface.

Alternatively, get direct downloads from here. It's easy to identify your edition of PaperCut - you'll see it on the About tab or by checking the footer of your PaperCut admin login.

Q What products are impacted by these vulnerabilities?

See the 'Which components are impacted' or 'Which components are not impacted' rows in the table above for a detailed list.

Q What is PaperCut doing to assist customers?

PaperCut and its partner network has activated response teams to assist PaperCut MF and NG customers. Our service desks are manned 24/7 via our support page.

The security response team at PaperCut has been working with external security advisors to compile a list of unpatched PaperCut MF/NG servers that have ports open on the public internet. In addition to our email and in-app announcements to all customers, we've been using this list to proactively reach out to potentially exposed customers via multiple means from Wednesday afternoon (AEST) and are working 24/7 through the weekend.

Q When was the exploit first detected in the wild?

PaperCut received our first report from a customer of suspicious activity on their PaperCut server on the 18th April at 03:30 AEST / 17th April 17:30 UTC.

PaperCut has conducted analysis on all customer reports, and the earliest signature of suspicious activity on a customer server potentially linked to this vulnerability is 14th April 01:29 AEST / 13th April

be taken.

Q Where are the release notes for these fixes?

You can see the release notes pages for PaperCut MF and NG which list all fixes included per version:

- MF - 20.1.7, 21.2.11, 22.0.9
- NG - 20.1.7, 21.2.11, 22.0.9

Q What are the CVSS scores for these vulnerabilities?

Vulnerability: CVE-2023–27350 / ZDI-CAN-18987 / PO-1216 / ZDI-23–233

- Score: 9.8 (Critical)
- Breakdown: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Vulnerability: CVE-2023–27351 / ZDI-CAN-19226 / PO-1219 / ZDI-23–232

- Score: 8.2 (High)
- Breakdown: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N

Q Do the current releases cover the new exploit method from VulnCheck and mentioned in the Bleeping Computer article, 6 May?

Yes, the New PaperCut RCE exploit created that bypasses existing detections article is referring to exploiting the same vulnerability, in a way that the activity is not easily detected in the Sysmon or PaperCut MF application log. The method of exploiting PaperCut MF mentioned in the article is mitigated in versions 20.1.7, 21.2.11, and 22.0.9 and later.

Q Is there more information available about these vulnerabilities?

Not at this time - to give customers a chance to upgrade, we are not releasing further details about these vulnerabilities.

If we can't upgrade to security patch, what other options are there?

Particularly if you have an older application version that doesn't have a minor patch available, we highly recommend locking down network access to the server(s).

- Block all inbound traffic from external IPs to the web management port (port 9191 and 9192 by default)
- Block all traffic inbound to the web management portal on the firewall to the server. Note: this will prevent lateral movement from internal hosts but management of the PaperCut service can only be performed on that asset.
- Apply "Allow list" restrictions under Options > Advanced > Security > Allowed site server IP addresses. Set this to only allow the IP addresses of verified Site Servers on your network. Note this only addresses ZDI-CAN-19226 / PO-1219

How do I know if my server has been exploited?

We currently recommend looking for the following Indicators of Compromise (IOCs) to determine if it is likely that the vulnerability has been used to install malware on the system. Depending on your systems, logging and endpoint protection software you may be able to detect the following.

- If you see suspicious activity or security alerts in Antivirus, anti-malware and endpoint security software tooling.
- If you see suspicious PaperCut MF application log entries, ie:
  - User "admin" logs into the administration interface
  - Admin user "admin" modified the print script on the printer
  - User "admin" updated the config key "…" (where the config key is not one you've deliberately changed)
  - User "[setup-wizard]" modified a config key
  - If your Application Server server logs happen to be in debug mode, check to see if there are lines mentioning `SetupCompleted` at a time not correlating with the server installation or upgrade.

- upd488[.]windowservicecemter[.]com/download/ld.txt
- upd488[.]windowservicecemter[.]com/download/AppPrint.msi
- upd488[.]windowservicecemter[.]com/download/a2.msi
- upd488[.]windowservicecemter[.]com/download/a3.msi
- anydeskupdate[.]com
- anydeskupdates[.]com
- netviewremote[.]com
- updateservicecenter[.]com
- windowcsupdates[.]com
- windowservicecentar[.]com
- windowservicecenter[.]com
- winserverupdates[.]com
- study[.]abroad[.]ge
- ber6vjyb[.]com
- 5[.]188[.]206[.]14
- upd488[.]windowservicecemter[.]com/download/update.dll

- New suspicious entries in SSH authorized keyfile.
- New print scripts in the setup. Review the 'Scripting' configuration of each printer (and device) in PaperCut MF/NG admin.
- SHA256 hashes of files on local system:
  - setup.msi f9947c5763542b3119788923977153ff8ca807a2e535e6ab28fc42641983aabb
  - ld.txt c0f8aeeb2d11c6e751ee87c40ee609aceb1c1036706a5af0d3d78738b6cc4125
- Powershell Scripts having similar content to:

```
-OutFile "setup.msi"

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

- Detection via YARA Rule on SIEM:

```
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
```

Additional context on the IoC may also be found in the CISA Advisory.

If you suspect that your server has been compromised, we recommend taking server backups, then wiping the Application Server, and rebuilding the Application Server and restoring the database from a

We will update this question with more details as we find more information from our customer base and security community.

How do I retain my data when restoring my Application Server?

Depending on how far back you need to restore your backup from, you may want to restore balances or other data changes in the gap between the last safe backup, and now.

There's some options for the restore process and subsequent data retention below:

1. Restore App Server and Database to a clean backup (**Recommended option**)
    - This would involve restoring the Application Server and database from a 'safe' backup point prior to when you discovered any suspicious behavior.
    - If you don't require the data changes between the safe backup and now, you're all set.

2. Restore App Server and Database, then update user balances (**Safe option**)
    - To restore recent user balances, we recommend restoring the latest (current) database backup containing all of the latest data, onto a staging machine that's running a patched version of the Application Server, and is not connected to the network. You can then use this environment to export your user balances, and then import them into the production (restored) system.
    - To export user balance / user credit data from your off-network system, run a user report - e.g. in the PaperCut MF/NG admin interface, head to **Reports > User > User reports > User list** then select the **CSV** report format. This will generate a list of your users and their current balances.
    - Then use the detailed information on the Batch import and update user data article to format the data into the correct columns, then import/update the data in your production system.

3. Restore App Server, and retain your most recent database
    - If you need to keep all your reporting data as well as user balance data and other changes to the database, you will need to manually clean a copy of your potentially compromised database.
    - We recommend restoring the latest (current) database backup containing all of the latest data, onto a staging machine that's running a patched version of the Application Server, and is not

- Set config key device.script.sandboxed is set to Y (the recommended default)
- Set config key print.script.sandboxed is set to Y (the recommended default)
- Delete any device scripts or print scripts which have been configured, in case they have been tampered with.
- Ensure that your user lists and other PaperCut MF/NG settings match with what you expect to see in your environment.

- Once you are confident that the staging machine settings are clean, perform a database export from the staging environment, then import that cleaned database data into the production environment.

Q Is there a maintenance release for versions 19 or older?

No - versions 19 and older are now “end of life”, as documented on our End of Life Policy page.

We recommend purchasing an updated license, which you can do online if you’re using PaperCut NG, or through your PaperCut Partner if you’re using PaperCut MF. You can find your PaperCut Partner contact information through the ‘About’ or ‘Help’ tab in the PaperCut administration interface.

Q I have a version 20 license, but no current M&S (maintenance and support) - can I still get this fix?

Yes! As long as you are running a version which is currently supported (version 20 or later) you can upgrade to whichever maintenance release version you’re licensed for. For example if you are licensed for version 20 but you don’t have a valid license for version 21, you can update to version 20.1.7 as above. See the ‘Where can I get the upgrade?’ question above for more details.

See our Upgrade Policy page for more information on licensing and upgrades.

Acknowledgements

PaperCut would also like to thank:

- "Huntress" team members Joe Slowik, Caleb Stewart, Stuart Ashenbrenner, John Hammond, Jason Phelps, Sharon Martin, Kris Luzadre, Matt Anderson and Dave Kleinatland.

Trend Micro have also advised they will disclose further information (TBD) about the vulnerability on 10th May 2023. For more information, see https://www.zerodayinitiative.com/advisories/published/ (filter on "PaperCut").

PaperCut Software would like to acknowledge and thank CISA for their Advisory published on 11th May 2023.

Security notifications

"How do I sign-up for paperCut's security mailing list?"

In order to get timely notifications of security news (including security related fixes or vulnerability information) please subscribe to our security notifications list via our Security notifications sign-up form. If you're a sys admin or if you look after PaperCut product implementations at your organization, this list will help you be amongst the first to hear of any security related news or updates.

Updates

Date	Update/Action
10th January 2023 (AEDT)	Vulnerability reported to PaperCut, by Trend Micro (see ZDI-CAN-18987 and ZDI-CAN-19226).

14th March 2023 (AEDT)	Trend Micro published additional details of the vulnerability on their website: ZDI-CAN-18987 and ZDI-CAN-19226.
19th April 2023 (AEST)	Updated this KB with new information discovered on the 18th April - indicating evidence to suggest that unpatched servers are being exploited in the wild.
20th April 2023 (AEST)	Published RCE security exploit in PaperCut servers blog post.
21st April 2023 (AEST)	Added “If we can’t upgrade to security patch, what other options are there?” (replaced the old “Is there a mitigation for these vulnerabilities if I don’t want to upgrade?”) Updated Acknowledgements section Updated “How do I know if my server has been exploited?”
22nd April 2023 (AEST)	Added new FAQ explaining what PaperCut has been doing to proactively support PaperCut MF and NG customers. Added new FAQ “When was the exploit first detected in the wild?”
23rd April 2023 (AEST)	No new updates - continuing to proactively reach out to customers with internet-facing servers.
24th April 2023 (AEST)	Added direct download links to ‘Where can I get the upgrade’
25th April 2023 (AEST)	Clarified that Multiverse and Print Logger are NOT impacted
27th April 2023 (AEST)	Minor clarifications to ‘not impacted’ section. Also listed each impacted or not-impacted version range explicitly

30th April 2023 (AEST)	No bulletin updates today. Reminder that the PaperCut support teams are on hand to assist customers with upgrading or mitigations if required.
2nd May 2023 (AEST)	Added 22.0.11 to the 'fixed' list, following today's release. Added the "How do I retain my data when restoring my Application Server?" question.
4th May 2023 (AEST)	Included the updated non-candidate ZDI reference numbers from Trend Micro (ZDI-23–233 and ZDI-23–232).
5th May 2023 (AEST)	Included a mention of Trinity Cyber, working with Trend Micro.
9th May 2023 (AEST)	Included a mention of Bleeping Computer article mentioning VulnCheck.
11th May 2023 (AEST)	Reverted mention of Trinity Cyber, working with Trend Micro.
12th May 2023 (AEST)	Added links to CISA Advisory.
16th May 2023 (AEST)	Added "22.0.9 and later" to fixed-versions list, since 22.0.12 is now out too.

Categories: FAQ , Security and Privacy

Keywords:

Last updated June 13, 2024

Customer stories

Testimonials

Print security

Integrations

Products at a glance

Forest positive

Best practices

Cookie settings