PaperCut NG/MF Security Bulletin (March 2026)

THE PAGE APPLIES TO:

PaperCut NG PaperCut MF PaperCut Pocket PaperCut Hive

Last updated March 31, 2026

Contents

With this release, we are evolving how we communicate security improvements to our community. Historically, our bulletins focused almost exclusively on high-impact vulnerabilities, providing a deep dive into specific issues. While we will continue this “deep dive” approach for major security events, we recognize that security is often built through a thousand small improvements.

To be more transparent, we are shifting to a more lightweight and frequent reporting format. This allows us to share the “everyday” security discoveries our teams stumble upon and fix (even in minor releases) that might not have met the high-impact threshold for a traditional bulletin in the past. This bulletin serves as a pilot for this new, more comprehensive reporting style.

It should be noted that the security mailing list would be still reserved for the high-impact security issues only, so we do not produce unnecessary noise on that channel.

Our Strategy: Beyond the Single Fix

At PaperCut, we believe that security is not a “set-and-forget” activity, but a continuous journey. This update is a direct result of our evolving strategy: rather than just fixing reported issues, we now task our development teams with “pattern hunting” – proactively searching our entire codebase for similar vulnerabilities whenever a new one is identified.

Proactive XSS Hardening

Recently, a minor Cross-Site Scripting (XSS) vulnerability was reported in the PaperCut NG/MF admin interface. While we moved immediately to patch this specific instance, we viewed it as an opportunity for a wider audit.

As part of our commitment to **secure-by-design** principles, our development team conducted a deep-dive research project across the PaperCut NG/MF codebase. This effort resulted in a **significant security uplift**, creating more robust handling of input fields across the application and hardening the product against future injection attacks using today’s

In parallel, our internal security research team has been auditing our embedded software. During a review of the **Konica Minolta** embedded application, one of our developers discovered an insecure communication channel between the device and the server that may occur under some model and setup combinations. This was identified and fixed internally under CVE-2026-5115 and proactively released into production builds ensuring customers have time to patch before public reporting.

Security issues addressed

CVE	Notes	CVSS rating and vector
CVE-2026-4794 Multiple cross-site scripting (XSS) vulnerabilities in PaperCut NG/MF	Following an internal research initiative to find and eliminate XSS patterns, PaperCut has implemented more robust input handling across the admin interface inline with best practices expected in 2026. **Vulnerability Type:** Cross-Site Scripting (XSS)	2.1 (LOW) CVSS:4.0 AV:N/AC:L/AT:P/PR:L/UI:P/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N

	admin's browser session. **Fixed in:** PaperCut NG/MF **25.0.10**	
CVE-2026-5115 Session hijacking in PaperCut NG/MF print pull or scan app for Konica Minolta	An internal audit revealed that a communication channel between the Konica Minolta embedded application and the PaperCut Application Server was insecure under certain conditions. **Vulnerability Type:** Session Hijacking / Information Disclosure **Impact:** Could potentially allow an attacker on the same local network to intercept sensitive data or mount a phishing attack	3.6 (LOW) CVSS:4.0 AV:A/AC:H/AT:N/PR:N/UI:P/VC:H/VI:N/VA:N/SC:H/SI:N/SA:N/E:U

MF **25.0.5** (Standard Release)

- PaperCut MF **25.0.9** (Konica Minolta Certified Release)

Who is impacted

You are likely impacted if you are running:

- **PaperCut NG/MF** versions prior to **25.0.10**.
- **PaperCut MF with Konica Minolta MFDs** using versions prior to **25.0.5** (Standard) or **25.0.9** (Certified).

Steps to resolve

PaperCut recommends that all customers upgrade to the latest version of PaperCut NG or MF inline with their upgrade cycle.

1. **Upgrade PaperCut NG/MF:** Install the latest build from the PaperCut website.
2. **Update Embedded Software:** For Konica Minolta fleets, ensure the embedded application is updated to the latest version after upgrading your Application Server.
3. **Verify Secure Connections:** Ensure that “Force HTTPS” is enabled in your PaperCut settings.

Minolta fix?

To ensure compatibility across different requirements, we maintain two distinct release tracks for Konica Minolta: a standard release and a version specifically certified by Konica Minolta. We have addressed the vulnerability in both tracks (**25.0.5** and **25.0.9**).

Q Can i resolve these vulnerabilities without upgrading?

No, these security improvements require code-level changes found only in the latest releases. To resolve these issues, you must upgrade to v25.0.10 for the XSS fixes (CVE-2026-4794), while the Konica Minolta fix (CVE-2026-5115) is available starting from v25.0.5 (Standard) or v25.0.9 (Certified).

Q Was there any evidence of these vulnerabilities being exploited?

No. These fixes have been applied through our internal security research and proactive auditing processes. They are not a response to any known exploits.

Security notifications

To stay informed about high impact security updates please subscribe to our Security notifications sign-up form.

Updates

Date	Update/action

Category: FAQ

Subcategory: Security and Privacy

HOW HELPFUL WAS THIS ARTICLE?

Not very helpful Very helpful

Comments

PaperCut

Subscribe to PaperCut communications

Email*

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.

Product overview

FEATURES

PaperCut MF/NG tour

PaperCut Hive/Pocket tour

FREE TOOLS

PaperCut Mobility Print

PaperCut QRDoc

BETA

In the Percolator

Life sciences

Legal

Small businesses

Large enterprise

Local government

WHAT OUR CUSTOMERS SAY

Customer stories

Testimonials

Blog

Resources

DISCOVER

Discover overview

WPP printing

Cloud and print

Easy printing

Remote printing

Print security

Integrations

Products at a glance

Forest positive

Best practices

ABOUT

About us

Careers

Security

B Corp

MISC

Become a PaperCut Reseller

Managed Service Provider Program

Privacy policy

Cookie settings