



Home > Support > Knowledge Base > [PaperCut NG/MF Security Bulletin \(March 2026\)](#)

# PaperCut NG/MF Security Bulletin (March 2026)

THE PAGE APPLIES TO:



Last updated March 31, 2026

## Contents

- Overview
- A New Approach to Security Transparency**
- Our Strategy: Beyond the Single Fix
- Security issues addressed
- Who is impacted
- Steps to resolve
- FAQs
- Security notifications
- Updates





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	<p>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.</p> <p><b>Vulnerability Type:</b> Cross-Site Scripting (XSS)</p>	<p>2.1 (LOW)</p> <p>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</p>



admins  
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.

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

**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



PaperCut  
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 in 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
31 March, 2026 (AEST)	Published the initial Security Bulletin.



Category: [FAQ](#)

Subcategory: [Security and Privacy](#)

### HOW HELPFUL WAS THIS ARTICLE?



Not very helpful

Very helpful

## Comments

We were unable to load Disqus. If you are a moderator please see our [troubleshooting guide](#).



Subscribe to PaperCut communications



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.

**PRODUCTS**

- PaperCut MF
- PaperCut NG
- PaperCut Hive
- PaperCut Pocket
- Product overview

**FEATURES**

- PaperCut MF/NG tour
- PaperCut Hive/Pocket tour

**FREE TOOLS**

- PaperCut Mobility Print
- PaperCut QRDoc

**BETA**

- In the Percolator

**SOLUTIONS FOR INDUSTRIES**

- High school/K-12
- Higher education
- Healthcare
- Coworking
- Life sciences
- Legal
- Small businesses
- Large enterprise
- Local government

**WHAT OUR CUSTOMERS SAY**

- Customer stories
- Testimonials

**SUPPORT**

- Support overview

**LEARN MORE**

- Interactive demos
- 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

**GET PAPER CUT**

- Contact Sales
- Book a demo
- How to buy

**ABOUT**

- About us
- Careers
- Security

- B Corp

**MISC**

- Become a PaperCut Reseller
- Managed Service Provider Program
- Privacy policy
- Cookie settings



Global-Mark.com.au

®

Corporation

PaperCut, the P symbol, and PaperCut products are trademarks of the PaperCut group of companies.

© PaperCut Software Pty Ltd