Actively Exploited PaperCut NG and MF Zero-Day Affects All Versions

Author: *Portia S. Cole – CTI Researcher*

TL;DR

Attackers are actively exploiting a zero-day vulnerability affecting all versions of PaperCut NG and PaperCut MF. PaperCut has confirmed customer incidents and released emergency patches for versions 25 and 26. A CVE, CVSS score and technical details have not been released.

Organizations should immediately restrict public access to affected Application Servers and install the emergency patch.

Overview

There is an actively exploited zero-day vulnerability in all versions of PaperCut NG and PaperCut MF. PaperCut has not disclosed how the vulnerability works, whether authentication is required or what level of access an attacker can gain. A CVE and CVSS score have not been assigned.

PaperCut NG and MF are print management platforms used to monitor printing, manage printers and multifunction devices, enforce printing policies and control access to printing and scanning features. Organizations can also use the platforms for secure print release, print archiving and document scanning.

PaperCut confirmed that attackers have exploited the vulnerability against customers. Information from a university customer's security and incident response teams allowed PaperCut to reproduce the flaw and develop an emergency fix.

Emergency patches are available for versions 25 and 26. PaperCut is still developing a patch for version 24. The company has not identified the threat actors responsible or disclosed what they are doing after compromising affected servers.

Affected Products

The vulnerability affects all versions of the following products:

- All versions of PaperCut NG are affected.
- All versions of PaperCut MF are affected.

PaperCut released the following emergency builds:

- PaperCut MF version 26.0.4, build 76494
- PaperCut MF version 25.0.12, build 76496
- PaperCut NG version 26.0.4, build 76495
- PaperCut NG version 25.0.12, build 76497

Published on: 8/27/2026

A patch for version 24 is still being developed. Organizations running older versions should upgrade to a patched version whenever possible.

Impact on Aspire Customers

Aspire customers may use PaperCut to manage printing, scanning, secure print release and multifunction devices across schools, healthcare facilities, government offices and other business environments.

Successful exploitation could allow an attacker to compromise the PaperCut Application Server. This could disrupt printing and scanning services or provide an entry point for additional activity within the customer's network. Environments that use Print Archiving may also store copies of printed or scanned documents on the server, although PaperCut has not confirmed that attackers have accessed or stolen data.

Customers with internet-accessible Application Servers face the highest risk. The currently available indicators are limited, which means organizations cannot rely on their absence to determine that a server has not been compromised.

The Common Vulnerability Scoring System (CVSS) rates vulnerabilities from 0 to 10 based on exploitability and potential impact.

- None (0.0): No severity
- Low (0.1–3.9): Limited impact
- Medium (4.0–6.9): Moderate risk
- High (7.0–8.9): Serious impact
- Critical (9.0–10.0): Severe impact requiring urgent attention

Aspire Protects

- Install the appropriate emergency build for PaperCut NG or PaperCut MF version 25 or 26. See PaperCut's security advisory for further details.
- Immediately restrict PaperCut Application Server web interfaces to trusted internal IP addresses. Firewall rules, network access controls or equivalent measures should prevent access from untrusted internet addresses.
- Upgrade older installations to a patched version whenever possible. Organizations that cannot upgrade should restrict access to the Application Server while waiting for an applicable patch.
- Review endpoint security, intrusion detection and network monitoring alerts involving the PaperCut Application Server.

- Investigate suspicious post-exploitation activity originating from pc-app.exe. This is a legitimate PaperCut process and should not be treated as malicious without additional evidence.
- Review server.log for unexpected truncation, deletion or the error messages listed in the Indicators of Compromise section.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190]: Threat actors are exploiting the vulnerability against PaperCut NG and MF Application Servers. Servers with web interfaces accessible from the public internet face the greatest risk.

IoCs

PaperCut identified the following **potential** indicators of compromise:

Process Activity

- Suspicious post-exploitation activity originating from pc-app.exe may indicate that an Application Server was compromised.

Note: The presence of pc-app.exe alone is not an indicator of compromise because it is a legitimate PaperCut process.

Log File Activity

- A missing server.log file may indicate compromise.
- An unexpectedly truncated server.log file may indicate compromise.
- A deleted server.log file may indicate compromise.

Log Entries
The following entries in server.log may indicate exploitation:

- ERROR No suitable driver found for jdbc:no:x
- ERROR DatabaseUtils - Database error looking up cardID: VALUES CAST

Targeted Industries

PaperCut NG and MF are widely used in industries that manage large printing environments, including:

- Education
- Healthcare
- Legal
- Public Sector

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company's reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.
- **NOC Services Notice**
  - If you are an Aspire NOC customer and are affected by these vulnerabilities, Aspire will open a case on your behalf. Customers interested in NOC services should contact Aspire's Customer Success Management team.

Supporting Documentation

URGENT Security Advisory: PaperCut NG/MF Security Bulletin (27 Aug 2026) | PaperCut