Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

PaperCut NG/MF Zero-Day Under Active Exploitation Across All Versions

Date of Publication	Admiralty Code	TA Number
August 28, 2026	A1	TA2026253

Summary

First Seen: August 27, 2026
Affected Products: PaperCut NG, PaperCut MF
Impact: PaperCut has confirmed active zero-day exploitation of two now-published flaws affecting all versions of PaperCut NG and MF. CVE-2026-82078 (Unsafe Dynamic Class Loading, CWE-470; CVSS 9.4) executes arbitrary code on the server but requires control of configuration parameters, CVE-2026-81578 (Authentication Bypass, CWE-306; CVSS 8.8) supplies exactly that, letting an unauthenticated attacker alter configuration. Chained, CVE-2026-81578 for entry, CVE-2026-82078 for code execution, they may yield unauthenticated RCE against internet-exposed Application Servers. Confirmed exploitation exists, and PaperCut urges restricting the web interface to trusted IPs and installing Emergency Patch Release 2 (v24/v25/v26, including Site and secondary servers). Given PaperCut's history as a recurring initial-access target, any exposed or unpatched server should be treated as at risk.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-82078	PaperCut NG and PaperCut MF Unsafe Dynamic Class Loading Vulnerability	PaperCut NG and PaperCut MF	✓	✗	✓
CVE-2026-81578	PaperCut NG and PaperCut MF Authentication Bypass Vulnerability	PaperCut NG and PaperCut MF	✓	✗	✓

Vulnerability Details

#1

PaperCut Software has confirmed that attackers are actively exploiting two vulnerabilities, CVE-2026-81578 and CVE-2026-82078, in its PaperCut NG and PaperCut MF print management software, and is treating the incident as its highest priority. The company's security response team is investigating confirmed user incidents. Both vulnerabilities affect all versions of both products, making the version number irrelevant to exposure. PaperCut's security team reproduced the vulnerabilities using information provided by a university user's internal security and digital forensics team, which is also how it confirmed they were being actively exploited in the wild, establishing this as a zero-day at the point of disclosure.

#2

The exploitation path is a two-vulnerability chain, CVE-2026-81578 (Authentication Bypass, CWE-306; CVSS 8.8) lets an unauthenticated attacker trigger administrative backend actions before access-validation completes and modify system configuration, while CVE-2026-82078 (Unsafe Dynamic Class Loading, CWE-470; CVSS 9.4) executes arbitrary Java bytecode on the server but requires the configuration control that CVE-2026-81578 provides, chained, they yield an unauthenticated remote code execution path, as reproduced by external researchers. PaperCut has not stated who is behind the attacks, what they do post-compromise, or whether data is being stolen.

#3

The indicators shared so far are behavioral and log-based rather than atomic artifacts. One should watch suspicious activity from the legitimate pc-app.exe process, and server.log files that are modified, deleted, or missing, plus two error strings referencing a JDBC driver failure and a cardID lookup error. The JDBC driver-failure string aligns with CVE-2026-82078's database-connector class-loading path, tying that indicator to the code-execution stage of the chain. The log tampering suggests anti-forensic activity, and the vendor warns their absence does not rule out compromise.

#4

PaperCut released an initial emergency out-of-cycle patch for the v25 and v26 branches (Windows, Linux, macOS) at 2:10 a.m. AEST on 28 August 2026, then published Emergency Patch Release 2 later the same day, extending coverage to the v24 branch and adding hardening developed with external researchers. Release 2 supersedes the original patch and should be installed even where the first was already applied, and Site Servers and secondary/print servers must be updated as well, not only the primary Application Server. Priorities are twofold: restrict the web interface to trusted addresses, and install Release 2 immediately.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-82078	All versions of PaperCut NG and PaperCut MF	cpe:2.3:a:papercut:papercut_ng:*:*:*:*:*:*:*:*, cpe:2.3:a:papercut:papercut_mf:*:*:*:*:*:*:*:*	CWE-470
CVE-2026-81578			CWE-306

Recommendations

Restrict Application Server Exposure Immediately: If your PaperCut NG/MF Application Server is reachable from the public internet, immediately restrict access to its web interfaces so they can be reached only from trusted IP addresses, such as internal networks. Use firewall rules, network access controls, or equivalent measures to ensure the server's web interfaces cannot be reached from untrusted internet addresses. Take this step now even if no suspicious activity has been observed, because the absence of warning signs does not confirm that a system is safe.

Apply Emergency Patch Release 2: Install PaperCut's Emergency Patch Release 2 without delay. Release 2 is now available for the v24, v25, and v26 branches of both NG and MF across Windows, Linux, and macOS, and includes additional hardening developed with external researchers. It supersedes the original emergency patch, install it even if you already applied the first patch. Update Site Servers and secondary/print servers as well, not only the primary Application Server; Print Deploy and Mobility Print are not affected. Verify each installer against the SHA256 checksum published in the bulletin before applying, and upgrade to the latest available version wherever feasible.

Check External-Database Card/ID Lookup Configuration: If your install uses an external database for Card/ID number lookups, review the vendor FAQ before and after patching. Where the feature is required, add security.card-number-lookup.enabled=Y to server/security.properties and restart the Application Server; the default is off, and without this key PaperCut silently ignores external lookup calls even if the Admin UI still shows the feature as configured.

Preserve Logs and Assume Breach for Exposed Servers: Because attackers have been observed tampering with server.log, protect and back up existing logs and forward them off-host to a SIEM or central log store before they can be altered, so evidence is preserved for investigation. Treat any Application Server that has been exposed to the internet as potentially compromised until proven otherwise, and initiate your incident response process for those hosts rather than relying solely on patching.

Strengthen Monitoring and Detection: Ensure the PaperCut Application Server is covered by endpoint detection, intrusion detection, and log monitoring, and create detections for the vendor-provided log strings and for anomalous behavior originating from the PaperCut application process. Continue to check the vendor advisory, as PaperCut has stated it will publish validated indicators of compromise and additional remediation guidance as its investigation matures.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	
Defense Evasion	T1070: Indicator Removal	
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Indicators of Compromise (IOCs)

TYPE	VALUE
Log Artifact	ERROR No suitable driver found for jdbc:no:x, ERROR DatabaseUtils - Database error looking up cardID: VALUES CAST

Patch Link

https://www.papercut.com/kb/Main/security-bulletin-27-aug-2026-urgent-security-advisory/

References

https://www.papercut.com/kb/Main/security-bulletin-27-aug-2026-urgent-security-advisory/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

August 28, 2026 • 07:30 AM

More at www.hivepro.com