



TLP: CLEAR

CALIFORNIA CYBERSECURITY INTEGRATION CENTER



CYBER ADVISORY

Monday, August 31, 2026

CAL-CSIC-202608-A-008

Chained Zero-Day Vulnerabilities Impacting Papercut NG and Papercut MF

Pre-Auth Remote Code Execution

Internal Pivoting

Java Code Execution

Emergency Patch Available

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of two zero-day vulnerabilities currently being exploited, being chained together to achieve remote code execution (RCE) against all versions of Papercut NG and Papercut MF – both of which are utilized as print management software. CVE-2026-81578 carries a CVSS 4.0 score of 8.8¹, while CVE-2026-82078 carries a CVSS 4.0 score of 9.4.²

CVE-2026-81578 is an authentication bypass vulnerability that permits an unauthenticated attacker with the ability to send HTTP requests through a web management interface to invoke certain administrative permissions before the targeted system completes its access validation. Successful exploitation would allow the attacker to alter system configuration settings without authentication.

CVE-2026-82078 is an Unsafe Dynamic Class Loading Vulnerability that allows an attacker with the ability to manipulate system configuration settings to create arbitrary database driver classes that would lead to arbitrary Java code execution. Successful exploitation allows a threat actor to access sensitive data and credentials, system-level access, and the potential to move laterally and pivot internally to other network segments. When chained together with CVE-2026-81578, they enable pre-authentication RCE within the PaperCut Application Server.³

PaperCut has acknowledged the vulnerability and has issued emergency patches for PaperCut NG and MF versions 24, 25 and 26. Their engineering team continues to work on an official release to address these vulnerabilities. Additionally, PaperCut has disclosed mitigation instructions with possible Indicators of Compromise.⁴ Both CVE-2026-80278 and CVE-2026-81578 were placed in CISA's Known Exploited Vulnerabilities catalog.

The Cal-CSIC recommends following PaperCut's mitigation guidance and installing their emergency patches as soon as possible.

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR

For additional details regarding both CVEs, please use this link:

PaperCut Security Advisory: <https://www.papercut.com/kb/Main/security-bulletin-27-aug-2026-urgent-security-advisory/#emergency-patch-release-2>

Affected Products and Versions

Product	Affected Version	Unaffected Version
All Versions of PaperCut NG and PaperCut MF are impacted		

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: [California Cybersecurity Integration Center | California Governor's Office of Emergency Services](#)

References

¹ OpenCVE; "CVE-2026-81578"; <https://app.openCVE.io/cve/CVE-2026-81578>; accessed 31 August 2026

² OpenCVE; "CVE-2026-82078"; <https://app.openCVE.io/cve/CVE-2026-82078>; accessed 31 August 2026

³ Huntress; "PaperCut Actively Exploited: A Pre-Auth RCE Chain"; <https://www.huntress.com/blog/papercut-actively-exploited>; accessed 31 August 2026

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR

⁴ PaperCut; "URGENT Security Advisory: PaperCut NG/MF Security Bulletin (27 Aug 2026)"; <https://www.papercut.com/kb/Main/security-bulletin-27-aug-2026-urgent-security-advisory/#who-is-potentially-impacted>; accessed 31 August 2026

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR