An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2609020277

NCSC Advisory

Zero-Day Vulnerabilities in PaperCut MF/NG

CVE-2026-81578 and CVE-2026-82078

2nd, September 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

CVE IDs: CVE-2026-81578 and CVE-2026-82078

Published: 2026-08-28

Vendor: PaperCut

Product: PaperCut MF/NG

CVE-2026-81578 CVSS Score[1]: 8.8

CVE-2026-82078 CVSS Score: 9.4

Products Affected

Product	Version
PaperCut MF/NG	0 < 24.1.10, 25.0.13, 26.0.5

Impact

CVE-2026-81578

An improper access control vulnerability exists in the web management interface of PaperCut MF and PaperCut NG. Under specific conditions, unauthenticated remote requests targeting administrative functions can trigger backend actions prior to the completion of access validation checks. This allows an unauthenticated remote attacker to modify certain system configurations.

Common Weakness Enumeration (CWE)[2]: CWE-305 Authentication bypass by primary weakness

Known Exploited Vulnerability (KEV) catalog[3]: Yes

Used by Ransomware Operators: N/A

[1] https://www.first.org/cvss/
[2] https://cwe.mitre.org
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

CVE-2026-82078

An unsafe dynamic class loading vulnerability exists in the database connection utilities of PaperCut MF and PaperCut NG. The application instantiates database driver classes based on configurable driver names without validating against an allowlist of approved drivers.If an attacker can manipulate system configuration parameters, this enables the execution of arbitrary Java bytecode residing on the application classpath under the security context of the PaperCut server process.

Common Weakness Enumeration (CWE): CWE-470 Use of Externally-Controlled input to select classes or code ('unsafe reflection')

Known Exploited Vulnerability (KEV) catalog: Yes

Used by Ransomware Operators: N/A

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from PaperCut.

- https://www.papercut.com/kb/Main/security-bulletin-27-aug-2026-urgent-security-advisory/
- https://github.com/rapid7/metasploit-framework/pull/21842

CVE-2026-81578

- https://nvd.nist.gov/vuln/detail/CVE-2026-81578
- https://www.cve.org/CVERecord?id=CVE-2026-81578
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-81578

CVE-2026-82078

- https://nvd.nist.gov/vuln/detail/CVE-2026-82078
- https://www.cve.org/CVERecord?id=CVE-2026-82078
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-82078