**GOVERNMENT OF THE REPUBLIC OF VANUATU**

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

**GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU**

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

2 September 2026

**Advisory 219: PaperCut NG/MF Authentication Bypass and Unsafe Dynamic Class Loading Remote Code Execution Vulnerabilities (CVE-2026-81578, CVE-2026-82078).**

**Release Date:** 28th August 2026
**Impact:** CRITICAL
**TLP:** CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that operate PaperCut NG or PaperCut MF print management software, including schools, hospitals, and government or office IT environments. This alert is intended to be understood by technical users and systems administrators.

# What is it?

CVE-2026-81578 and CVE-2026-82078 are two critical vulnerabilities in PaperCut MF and PaperCut NG that CERTVU is addressing together because they share the same fix and are being actively chained by attackers.

**CVE-2026-81578** is an authentication bypass in the web management interface: under specific conditions, an unauthenticated remote attacker can send requests targeting administrative functions that trigger backend actions before access validation completes.

**CVE-2026-82078** is a separate flaw in PaperCut's database connection utilities, caused by unsafe dynamic loading of Java classes, that lets an attacker who can influence the class reference cause PaperCut to load and execute arbitrary Java code.

# What are the systems affected?

The following version(s) are affected (both CVEs):

- PaperCut MF and PaperCut NG versions before 24.1.10, 25.0.13, and 26.0.5 – (Affected)
- PaperCut MF and PaperCut NG version 23.x and earlier – (Affected, and no patch is currently available for this version line)

PaperCut MF and PaperCut NG 24.1.10, 25.0.13, 26.0.5 and later – (Not affected, patched)

A single PaperCut emergency patch release fixes both CVE-2026-81578 and CVE-2026-82078; there is no need to apply separate updates.

# What does this mean?

**Typical attack flow:**

1. **Bypass authentication (CVE-2026-81578)**
    - An attacker sends an unauthenticated request directly to an administrative function on the PaperCut web management interface; the backend executes the action before its access validation check completes, granting the attacker admin-level access with no credentials.
2. **Escalate to remote code execution (CVE-2026-82078)**
    - Using that access, the attacker reaches PaperCut's database connection configuration and supplies a crafted class reference, causing PaperCut to dynamically load and execute arbitrary Java code.

**Attack vectors:**

- Fully unauthenticated, chained exploitation of both CVEs together - the scenario CERTVU considers most likely and most dangerous.
- Exploitation of CVE-2026-82078 alone by an attacker who already holds valid or stolen administrative credentials to the PaperCut management interface.

Successful exploitation may allow attackers to:

- Modify PaperCut system configuration without authentication.
- Execute arbitrary code on the PaperCut application server, including deploying remote access tools, without needing any valid credentials at all.

# Mitigation process

CERTVU recommends the following:

1. Apply PaperCut's emergency patch immediately

- Upgrade to PaperCut MF/NG 24.1.10, 25.0.13, or 26.0.5 (or later) without delay. This single patch release addresses both CVE-2026-81578 and CVE-2026-82078.

2. Upgrade unsupported version 23.x or earlier installations
3. Restrict access to the management interface
4. Audit the estate for the affected product
5. Conduct a compromise assessment

Report suspected compromise to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

# Reference


1. https://www.papercut.com/kb/Main/PC-CVE-2026-81578
2. https://www.papercut.com/kb/Main/PC-CVE-2026-82078
3. https://www.cve.org/CVERecord?id=CVE-2026-81578
4. https://www.cve.org/CVERecord?id=CVE-2026-82078
5. https://www.cisa.gov/known-exploited-vulnerabilities-catalog