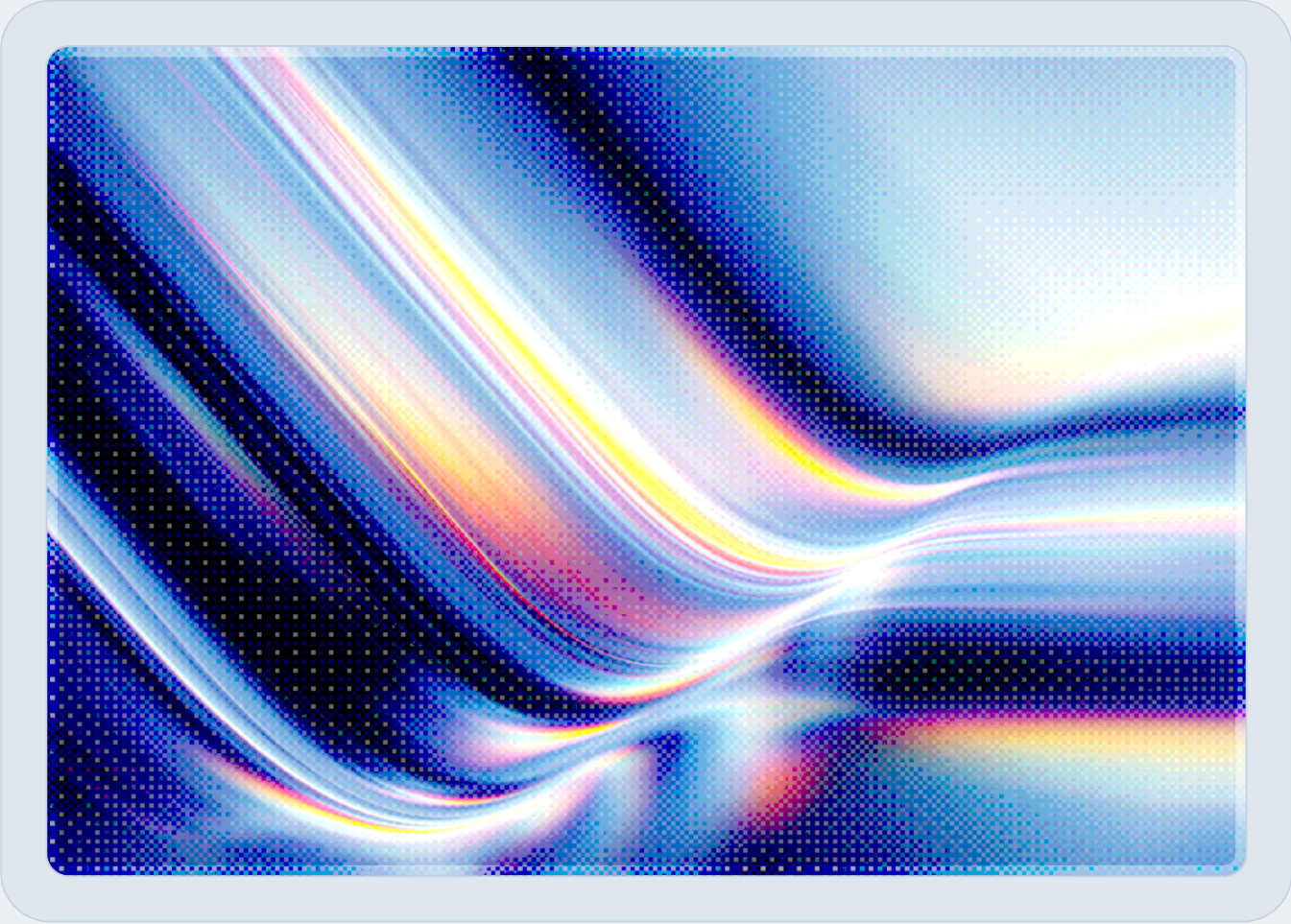
CSAI Foundation | Cloud Security Alliance

Chained PaperCut Flaws Enable Education-Sector Credential Theft

2026-09-06

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Key Takeaways

Threat actors are actively chaining two PaperCut NG/MF vulnerabilities — CVE-2026-81578, a missing-authentication flaw in the web management interface, and CVE-2026-82078, an unsafe reflection bug in the database connection utilities — to gain unauthenticated remote code execution against print management servers, with confirmed intrusions against K-12 schools and universities across the United States and Europe [1][2]. PaperCut disclosed active exploitation on August 27, 2026, and the Cybersecurity and Infrastructure Security Agency (CISA) added both CVEs to its Known Exploited Vulnerabilities (KEV) catalog four days later, on August 31 [3][4]. Arctic Wolf's Adversary Research Team has since documented a hands-on-keyboard campaign in which attackers used the chain to create rogue administrator accounts, dump Windows registry hives to extract the SAM database BootKey, and stage Metasploit/Meterpreter payloads for follow-on access [1][2]. Because PaperCut servers are typically integrated with Active Directory or LDAP for print authentication, a compromise of the application can cascade into domain-wide credential exposure — a risk profile that education IT environments, which are often thinly staffed and slow to patch internet-facing infrastructure, are poorly positioned to absorb [1][5].

Background

PaperCut NG and PaperCut MF are widely deployed print management platforms used by schools, universities, government agencies, and enterprises to control and audit network printing, and both editions have a documented history of being targeted by opportunistic and ransomware-affiliated attackers. In 2023, CVE-2023-27350 — an authentication bypass in the same product line — was exploited by Bl00dy ransomware actors against U.S. education-sector organizations, prompting a joint CISA/FBI advisory at the time [6]; Microsoft separately attributed a parallel wave of exploitation against the same flaw to the Cl0p-affiliated Lace Tempest group [13]. The current incident echoes that pattern closely enough that CSA's own rapid-research team flagged the parallel when the new flaw first surfaced: in an August 28, 2026 research note published before CVE identifiers had even been assigned, CSA characterized the bug as "the second major authorization bypass in roughly three years" for PaperCut and noted that the vulnerability had been detected by a university's own incident response team rather than through vendor telemetry [7].

The current chain begins with CVE-2026-81578, which PaperCut describes as an improper access control flaw in the product's web management interface: a specifically crafted request can cause one internal component to render a response while a different, unintended component actually processes the underlying action, allowing an unauthenticated attacker to modify server configuration values [12]. That configuration tampering is then used to activate CVE-2026-82078, an unsafe dynamic class-loading vulnerability in the database connection utilities that lets an attacker load and execute arbitrary Java bytecode under the security context of the PaperCut Application Server process [12]. PaperCut assigned CVSS 4.0 scores of 8.8 to CVE-2026-81578 and 9.4 to CVE-2026-82078, reflecting the severity of a pre-authentication path to full server compromise [9][12]. Huntress, which reproduced the complete exploitation chain against a standard PaperCut NG installation, traced the earliest confirmed customer incidents to August 26, 2026, one day before the vendor's public advisory [8]. The vendor shipped an initial emergency patch for the 25.x and 26.x branches within roughly 24 hours of disclosure, followed by a second emergency release the same day to broaden hardening and add coverage for version 24, and a further "Release 3" build on September 1 that superseded the earlier fixes [8][9]. Huntress has also noted that of the roughly 2,500 PaperCut installations it tracks in its own customer base, close to half are running version 23 or older – releases for which no patch has yet been published – leaving a substantial population of servers with no vendor-supplied remediation path beyond removing internet exposure [8].

Security Analysis

The exploitation activity documented by Arctic Wolf and corroborated by other researchers shows a consistent, repeatable post-compromise sequence once an attacker has achieved code execution through the chain. Initial commands are typically basic host and identity reconnaissance – `whoami`, `ver`, `tasklist`, and `uname` – executed as child processes of PaperCut's `pc-app.exe`, a parent-process relationship that is itself a strong detection signal, since that binary rarely if ever has a legitimate reason to spawn a command shell [1][2]. Attackers observed in the education-sector campaign then created a new privileged local account named "Administrator17," a naming convention distinctive enough to function as a search term across endpoint logs [1][2]. From that foothold, they used the built-in Windows utility `certutil.exe` with URL-download flags to retrieve credential-harvesting tools – including `lsa_collect.exe`, `lsa_collect_small.exe`, and `save_hives.exe` – from attacker-controlled infrastructure at the IP addresses 45.142.193[.]132 and 194.180.48[.]134 [1]. Those tools extract the `HKLM\SAM`, `HKLM\SYSTEM`, and `HKLM\SECURITY` registry hives, which together allow recovery of the Windows BootKey and, from it, locally cached NTLM password hashes [1][2]. In parallel, attackers searched PaperCut configuration files for the strings "password," "secret," "ldap," "bind," and "token" – a direct attempt to recover the LDAP or Active

Directory service-account credentials that PaperCut servers commonly store to synchronize print users, which if successful would hand attackers a path from a single print-server compromise into the broader campus directory [1][2]. Some intrusions additionally deployed Java-based Meterpreter payloads to establish persistent remote command-and-control sessions [1][2].

Independent of the credential-theft campaign, Huntress has published forensic artifacts consistent with the exploitation chain itself, including base64-encoded reconnaissance commands, hex-encoded malicious Java `.class` files dropped with randomized names such as `Udydn.class` and `Moo97.class`, anomalous Derby database log entries referencing `jdbc:derby:memory:pwn`, and cases of the PaperCut `server.log` file being truncated or deleted outright — behavior consistent with an attacker attempting to remove evidence of the initial exploitation request [8]. The combination of a pre-authentication entry vector, a known and searchable persistence indicator ("Administrator17"), and a credential-harvesting objective aimed squarely at directory-service secrets distinguishes this campaign from simple opportunistic web-shell deployment. In CSA's assessment, this pattern points toward attackers who understand that PaperCut's typical deployment model — an internet- or campus-network-facing service account with LDAP bind privileges — makes it an efficient stepping-stone into identity infrastructure rather than an end target in itself.

The education sector's exposure to this campaign is not incidental, though this note has not independently verified the specific IT conditions at the schools and universities affected. K-12 districts and universities are commonly described in security-sector reporting as operating print-management and similar infrastructure that was provisioned years earlier by staff who have since departed, with limited network segmentation between administrative and instructional zones, and patched on academic-calendar cycles rather than in response to vendor severity ratings. Those structural conditions are consistent with why the sector was disproportionately represented among CVE-2023-27350 victims in 2023 [6], and CSA's assessment is that similar conditions plausibly explain this campaign's concentration in education as well — an inference that should be read as analytical judgment rather than a documented finding specific to the organizations affected here. CISA's decision to add both CVE-2026-81578 and CVE-2026-82078 to the KEV catalog within days of disclosure, invoking Binding Operational Directive 26-04's requirement that federal agencies remediate KEV-listed vulnerabilities on internet-facing assets on an accelerated, risk-tiered timeline, reflects the same urgency that Huntress and Arctic Wolf's private-sector telemetry independently support [3][4][14].

Recommendations

Immediate Actions

Organizations running PaperCut NG or MF should determine within hours, not days, whether their Application Server is reachable from the public internet or from an unsegmented internal network, and if so restrict access to trusted management IP ranges via firewall policy as an interim control while patching is arranged. Security teams should hunt existing logs for the specific indicators published by researchers: command shells (`cmd.exe`, `powershell.exe`) spawned as children of `pc-app.exe`; reconnaissance commands such as `whoami`, `ver`, `tasklist`, and `uname`; the account name "Administrator17" or other unexpected new local administrator accounts; `certutil.exe` invocations with download flags; and outbound connections to 45.142.193[.]132 or 194.180.48[.]134 [1][8]. Any PaperCut server showing these indicators should be treated as compromised and investigated for lateral movement toward Active Directory, given the campaign's demonstrated focus on harvesting directory-service credentials.

Short-Term Mitigations

Affected organizations should apply PaperCut's latest emergency patch build for their installed branch without delay, and should independently verify the applied version rather than relying solely on an update notification, echoing the "patch available versus patch applied" gap CSA first flagged in its ShareFile pre-auth RCE analysis [10] and has since observed recur in this PaperCut chain as well [7]. Because Huntress data indicates a substantial share of deployed installations run version 23 or earlier and currently have no vendor patch, administrators of those older branches should prioritize removing the server from direct network exposure and evaluate emergency upgrade to a supported branch. Wherever PaperCut integrates with LDAP or Active Directory, the associated service-account credentials should be rotated on the assumption that configuration files may have already been read by an attacker, and rotation should be treated as mandatory — not optional — for any instance that showed indicators of compromise.

Strategic Considerations

The recurrence of a second major PaperCut authentication-bypass chain within three years of CVE-2023-27350 argues for treating print management infrastructure as identity-adjacent rather than as a low-risk peripheral service, particularly in education environments where these servers routinely hold LDAP bind credentials with broad directory read access. Institutions should reassess whether print

servers require any direct network reachability beyond the print clients and administrative consoles that genuinely need it, and should build periodic exposure reviews of "boring" infrastructure — print management, badge systems, and similar utility services — into vulnerability management programs that otherwise focus attention on higher-profile applications. The pattern also reinforces the value of exploitation-informed prioritization over static CVSS scoring alone: both CVE-2026-81578 and CVE-2026-82078 moved from disclosure to CISA KEV listing in four days, and organizations that wait for a routine patch cycle to address KEV-listed flaws on internet-facing assets will consistently trail active campaigns.

CSA Resource Alignment

CSA's own August 28, 2026 rapid-research note, "PaperCut Zero-Day: Unauthenticated RCE Hits All NG/MF Versions", analyzed this exact vulnerability chain within a day of PaperCut's initial disclosure and before CVE identifiers had been assigned, correctly identifying it as a repeat of the authorization-bypass pattern seen in CVE-2023-27350 and recommending immediate restriction of Application Server internet exposure — guidance that this note's post-exploitation findings now confirm was well-founded, since exposed servers are precisely what the education-sector campaign has targeted [7]. Readers should treat that earlier note and this one as companion pieces: the first addresses the vulnerability mechanics and initial patch guidance, while this note documents the confirmed real-world exploitation and credential-theft objectives observed since.

CSA's analysis of the July 2026 Progress ShareFile incident, "ShareFile's Credible Threat: A Pre-Auth RCE Chain Explained", offers a directly comparable case study in the same vulnerability class: an authentication-bypass flaw chained with a second flaw to achieve unauthenticated remote code execution against internet-facing enterprise infrastructure, exploited in the wild within months of patch availability [10]. That note's core observation — that the gap between "patch available" and "patch applied" is where exploitation-informed vulnerability management earns its value over static CVSS scoring — is the framing CSA first developed there, and it applies directly to PaperCut's fragmented patch adoption across its installed base [10].

CSA's AI Controls Matrix (AICM) v1.1 is written for AI system governance rather than traditional infrastructure, but its Technology Vulnerability Management (TVM) domain articulates control objectives — exposure tracking, patch governance, and vulnerability lifecycle management — that are directly analogous to the exposure-review and exploitation-prioritization gaps this incident illustrates in a non-AI context [11]. Education-sector security teams building or maturing a vulnerability management program can use the TVM domain's control structure as a starting reference point for formalizing those practices, even though AICM was not written with conventional print-server infrastructure in mind.

References

[1] The Hacker News. "Attackers Exploit PaperCut Flaws to Steal Credentials From Schools and Universities." The Hacker News, September 5, 2026.

[2] Security Affairs. "PaperCut Flaws Exploited in Attacks on U.S. and European Schools." Security Affairs, September 5, 2026.

[3] Cybersecurity and Infrastructure Security Agency. "CISA Adds Two Known Exploited Vulnerabilities to Catalog." CISA, August 31, 2026.

[4] Security Affairs. "U.S. CISA Adds PaperCut NG/MF Flaws to Its Known Exploited Vulnerabilities Catalog." Security Affairs, August 31, 2026.

[5] SecurityWeek. "PaperCut Exploitation Escalates to Active Intrusions." SecurityWeek, September 1, 2026.

[6] CISA / FBI. "#StopRansomware: CVE-2023-27350 PaperCut MF/NG Vulnerability." CISA, May 12, 2023.

[7] Cloud Security Alliance. "PaperCut Zero-Day: Unauthenticated RCE Hits All NG/MF Versions." CSA Labs, August 28, 2026.

[8] Huntress. "PaperCut Zero-Day: Active Exploitation and Pre-Auth RCE." Huntress, August 2026.

[9] runZero. "PaperCut Software Vulns: CVE-2026-81578, CVE-2026-82078." runZero, August 31, 2026.

[10] Cloud Security Alliance. "ShareFile's Credible Threat: A Pre-Auth RCE Chain Explained." CSA Labs, July 14, 2026.

[11] Cloud Security Alliance. "AI Controls Matrix (AICM) v1.1." Cloud Security Alliance, 2026.

[12] PaperCut. "URGENT Security Advisory: PaperCut NG/MF Security Bulletin (27 Aug 2026)." PaperCut Knowledge Base, August 27, 2026.

[13] SecurityWeek. "Microsoft: Cl0p Ransomware Exploited PaperCut Vulnerabilities Since April 13." SecurityWeek, 2023.

[14] Cybersecurity and Infrastructure Security Agency. "Binding Operational Directive 26-04: Prioritizing Security Updates Based on Risk." CISA, June 10, 2026.