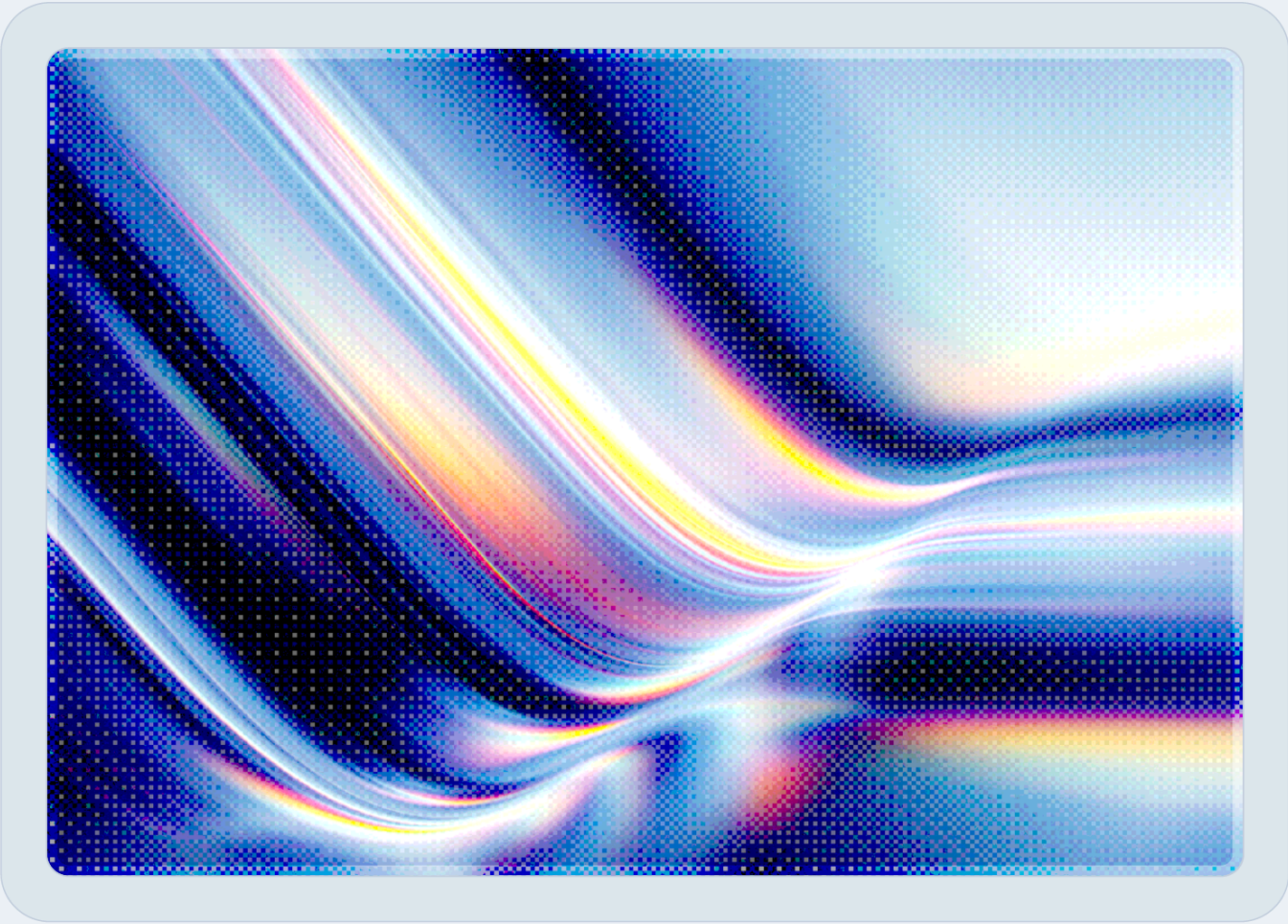
CSAI Foundation | Cloud Security Alliance

PaperCut Zero-Day: Unauthenticated RCE Hits All NG/MF Versions

2026-08-28

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Key Takeaways

PaperCut disclosed on August 27, 2026 that its NG and MF print management software is under active zero-day attack, with the vendor treating every currently supported version as potentially affected pending a full root-cause fix [1][2]. Confirmed customer incidents, first surfaced through a university's own security and forensics team, allowed PaperCut to reproduce and validate the flaw, and the company shipped emergency patches within roughly 24 hours of going public [1][3]. Independent analysis by Huntress indicates the bug is a pre-authentication remote code execution issue rooted in an authorization logic flaw that lets a crafted request confuse which page or component is actually processing it, echoing the mechanism behind PaperCut's last major incident in 2023 [4]. No CVE identifier had been assigned as of this writing, and PaperCut has withheld exploitation and payload details while the investigation continues, which narrows what defenders can independently verify [1][2]. Organizations running internet-facing PaperCut Application Servers should treat this as an emergency-patch, assume-compromise event: apply the available fixes for the 25.x and 26.x branches immediately, restrict web-interface access to trusted networks in the meantime, and hunt for the indicators of compromise PaperCut and Huntress have published [1][3][4].

Background

PaperCut NG and PaperCut MF are print management platforms widely deployed across higher education, K-12, healthcare, and enterprise print environments to track usage, enforce quotas, and manage authentication for shared printers and multifunction devices. Because these platforms sit at the intersection of identity, billing, and device management, their Application Server component typically runs with elevated privileges and is often exposed to the internet in practice, allowing students, patients, or remote staff to submit print jobs or manage accounts without a VPN. That combination of broad privilege and internet exposure has made PaperCut a recurring target: in March 2023, a critical improper-access-control flaw in the software's SetupCompleted class (CVE-2023-27350, CVSS 9.8) let unauthenticated attackers bypass authentication entirely and reach administrative functionality, a bug the FBI and CISA later tied to Bl00dy ransomware operators and other groups hitting the education sector specifically [5].

On August 27, 2026, PaperCut published an urgent security bulletin stating that it was aware of confirmed customer incidents involving a previously unknown vulnerability in NG and MF, and that it was "treating this matter with the highest priority" [1][2]. PaperCut declined to publish a CVE number, a CVSS score, or a description of the underlying flaw, citing the active and ongoing nature of the exploitation [1] — a more limited disclosure than PaperCut provided for its 2023 incident, where CVE-2023-27350 and a CVSS score were published alongside CISA's advisory [5]. According to BleepingComputer and Help Net Security, the company's security team was only able to reproduce the issue after a university customer's own incident response and digital forensics staff identified suspicious activity, investigated it, and shared their findings with PaperCut directly, a discovery path that shows PaperCut's own detection and monitoring did not independently surface the issue: the reproduction data instead came from a customer's incident response and forensics team [1][2]. PaperCut has since confirmed the vulnerability affects the Application Server component when it is reachable from the public internet, and by August 28 had released emergency, not-yet-fully-validated patches for the currently supported 25.x and 26.x release branches, with a fix for the older but still supported version 24 branch still in development [2][3][4].

Because PaperCut has withheld technical specifics, much of what is publicly known about the exploitation mechanism comes from independent research rather than the vendor's own advisory. Security firm Huntress, which monitors managed endpoints across a large base of small and midsize organizations, reported that it reconstructed a working proof-of-concept and observed the exploit chain in telemetry from its own customer base, giving the broader security community its clearest picture yet of how the attack actually unfolds [4]. That gap between what the vendor will confirm and what third-party researchers are independently observing means organizations should cross-reference multiple sources, including their own logs, rather than relying on a single authoritative technical writeup to assess exposure.

Security Analysis

Huntress's analysis describes the root cause as an authorization logic flaw in how PaperCut's web application routes requests: a specifically crafted request can reference one page for rendering purposes while a different page's component or action actually executes, allowing an unauthenticated request to trigger functionality that should require administrative access [4]. If accurate, this "page confusion" pattern is conceptually similar to the access-control bypass at the heart of CVE-2023-27350, where a request to the SetupCompleted class let an attacker skip authentication and reach the administrative interface directly [5]. That similarity does not necessarily mean the two flaws share code, but it does suggest PaperCut's web tier has a recurring class-of-bug problem around request routing and authorization checks that a single patch is unlikely to fully retire.

Once an attacker bypasses authorization, PaperCut's own architecture gives them a path to full code execution: the Application Server exposes configuration and printer-management functionality that can be repurposed to load and execute attacker-supplied Java code, similar to how the 2023 flaw was chained into remote code execution through legitimate product features such as printer scripting [4][5]. Huntress reported observing the PaperCut process (pc-app.exe on Windows) spawning follow-on processes consistent with reconnaissance commands, and both PaperCut and Huntress published indicators of compromise that defenders can search for now: missing, truncated, or otherwise altered server.log and derby.log files; database error entries reading "ERROR No suitable driver found for jdbc:no:x" and "ERROR DatabaseUtils - Database error looking up cardID"; and encoded strings in logs consistent with basic system-enumeration commands such as whoami and tasklist [1][3][4]. The presence of "cardID" in one of the flagged database error strings suggests the affected component may interact with card- or identity-linked print-quota records, a data pattern common in some PaperCut deployments that tie print quotas to student or badge IDs. Neither PaperCut nor Huntress has confirmed what data this specific field stores in the exploited instances, so organizations should verify their own PaperCut database schema and treat any confirmed payment-card or identity linkage as grounds for elevating incident severity beyond print-service disruption.

Because PaperCut has not disclosed whether the vulnerability requires the attacker to already have some form of network access or whether it is exploitable purely over an exposed web interface, organizations should assume the more dangerous case: a fully unauthenticated, internet-reachable pre-auth RCE, consistent with Huntress's characterization [4]. The vendor's own mitigation guidance points the same direction, advising customers with internet-facing Application Servers to immediately restrict access to trusted IP ranges via firewall rules or equivalent network controls rather than relying on application-layer authentication alone [1][2][3]. That advice is consistent with — though PaperCut has not confirmed — an authentication or authorization layer that cannot yet be trusted to stop an attacker who can reach the interface.

The emergency patches released for the 25.x and 26.x branches on August 27 and 28 close the immediate hole for supported deployments, but PaperCut has been explicit that version 24 fixes remain in progress and that its own understanding of the flaw is still evolving, meaning the patch content and scope could change as the investigation continues [2][3][4]. Organizations running end-of-life PaperCut releases predating version 24 appear to have no vendor remediation path based on PaperCut's public communications to date, and should treat continued internet exposure of those instances as an active, unmitigated risk requiring network isolation rather than a patch, pending confirmation from the vendor.

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, and if so, restrict access to known-trusted IP ranges through firewall rules, a VPN, or equivalent network access controls, exactly as PaperCut has advised [1][2][3]. Supported customers on the 25.x or 26.x branches should apply PaperCut's emergency patches (NG 25.0.12.76497 and MF 25.0.12.76496, or the corresponding 26.x builds) as soon as change-control processes allow, treating this as an emergency, out-of-cycle change [2][3][4]. While applying patches or restricting access, security teams should also search server.log and derby.log for the published indicators of compromise, including the "jdbc:no:x" and "cardID" database error strings, unexplained gaps or truncation in log files, and unexpected child processes spawned from the PaperCut Application Server process, and should treat any match as evidence of likely compromise requiring incident response rather than routine patching [1][3][4].

Short-Term Mitigations

Where public internet exposure cannot be eliminated quickly, for example because remote students, patients, or staff genuinely need to reach the print portal, organizations should evaluate placing the Application Server behind a reverse proxy or VPN gateway that enforces authentication before traffic ever reaches PaperCut itself, reducing the attack surface even if the underlying authorization bug is not yet fully understood. Because PaperCut's own advisory notes that its analysis and patch guidance are still evolving, security teams should subscribe to the vendor's security bulletin page and re-check patch status for version 24 and any other affected branches over the coming days rather than treating the initial emergency patch as the final word [2][3]. Given that the vulnerability appears rooted in a request-routing and authorization design pattern rather than a single line of vulnerable code, teams should also budget time for a second round of hardening once PaperCut publishes a fuller root-cause analysis and CVE, since a narrow patch addressing only the specific exploited path has, in this product's history, previously left related routes exploitable.

Strategic Considerations

This is the second time in roughly three years that a PaperCut authorization flaw has enabled unauthenticated remote code execution against internet-facing deployments. The 2023 incident was confirmed by CISA and the FBI to disproportionately affect the education sector [5]; whether the

current campaign shows a similar pattern is not yet established — the only education-sector detail confirmed so far is that a university's IR team was first to detect and report it [1][2]. Given PaperCut's tight coupling to student identity and card systems in many higher-education deployments, organizations in that sector should not assume they are a lower-priority target regardless of confirmed victim distribution. Organizations that depend on PaperCut, or similar centralized print, identity, and device-management platforms, should reassess whether those systems need direct internet exposure at all, and should apply the same exposure-reduction and network-segmentation logic to other identity-adjacent infrastructure that is often overlooked in vulnerability-management prioritization because it is not classified as a security tool. The compressed timeline in this case, from a customer-discovered incident to a vendor advisory to an emergency (if not fully validated) patch in roughly a day, also illustrates how little runway defenders now get between disclosure and exploitation, which is why CSA recommends organizations weight exposure reduction and detection engineering at least as heavily as patch velocity when defending internet-facing management-plane software.

CSA Resource Alignment

This incident's core failure mode, an unauthenticated, internet-facing management-plane flaw exploited before a CVE was even assigned, illustrates a dynamic in CSA's ongoing analysis of AI-era vulnerability discovery: organizations increasingly need to prioritize exploitability validation and exposure reduction over waiting for complete vendor disclosure, weighting environmental exposure and active-exploitation signals above formal severity scoring. That framing applies directly here, since PaperCut has not published a CVSS score at all, leaving KEV-style, exposure-based triage as the only realistic prioritization signal available to defenders right now. The pattern also echoes other recent unauthenticated, internet-facing zero-days against on-premises management-plane software, where organizations that moved beyond patching alone, rotating credentials and hardening detection in addition to applying the vendor's fix, were better positioned than those that treated the emergency patch as the end of the response. More concretely, the CSA AI Controls Matrix (AICM) v1.1 gives PaperCut operators a framework for translating this incident into documented, audit-ready controls: its Threat & Vulnerability Management and Application and Interface Security domains cover patch timeliness, network exposure controls, and detection coverage that operators can record for assurance purposes once the incident is resolved [6].

References

[1] Sergiu Gatlan. "PaperCut warns of NG, MF flaw exploited in zero-day attacks." BleepingComputer, August 27, 2026.

[2] Help Net Security. "Unknown PaperCut NG/MF vulnerability is under active attack." Help Net Security, August 27, 2026.

[3] The Register. "Print management outfit PaperCut is under 0-day attack, and it's drawing customers' blood." The Register, August 28, 2026.

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

[5] Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation. "Malicious Actors Exploit CVE-2023-27350 in PaperCut MF and NG." CISA Alert AA23-131A, May 11, 2023.

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

