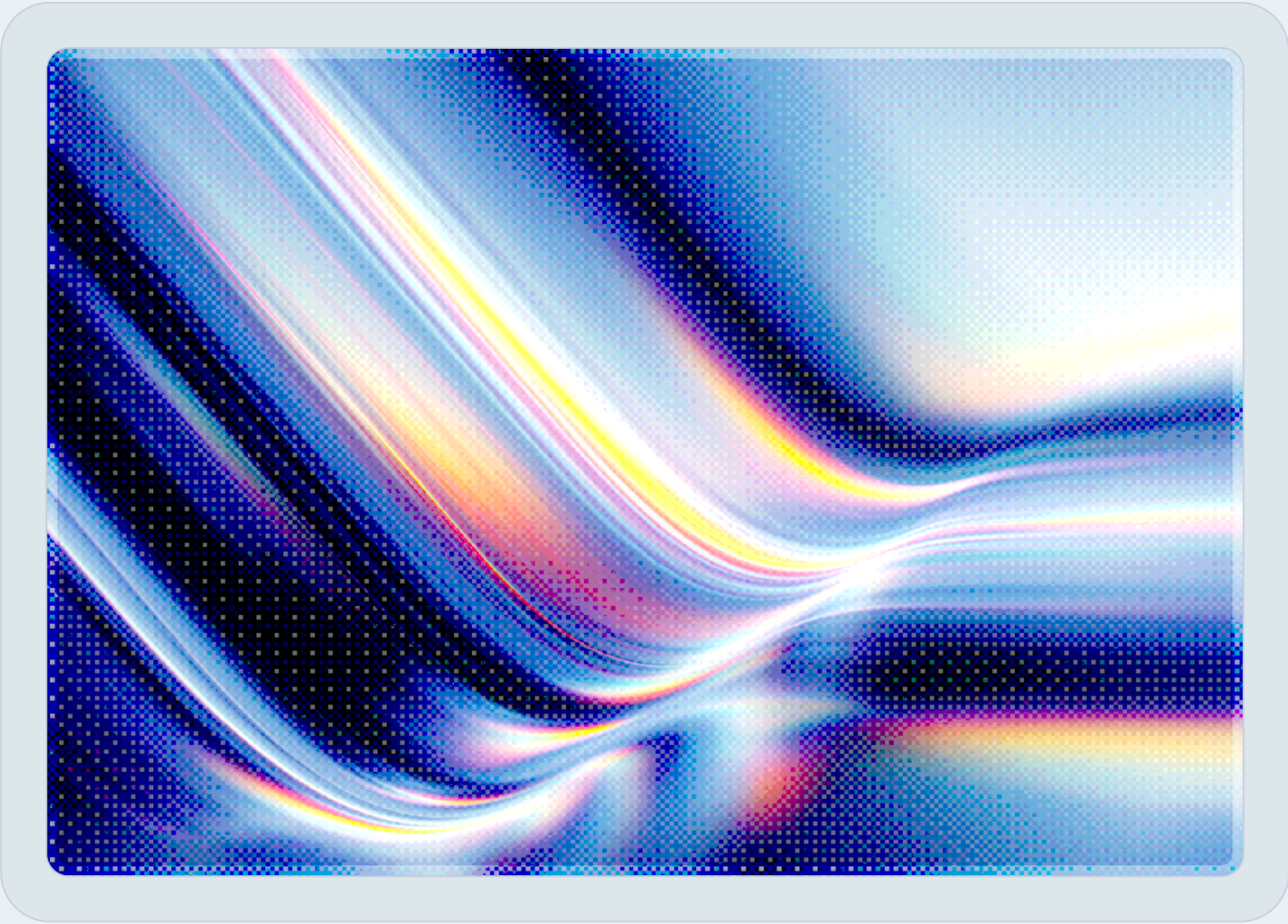
CSAI Foundation | Cloud Security Alliance

Citrix NetScaler Zero-Days Under Active Global Exploitation

2026-09-28

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Key Takeaways

Citrix disclosed eight NetScaler ADC and NetScaler Gateway vulnerabilities on September 27, 2026, and confirmed that two of them, CVE-2026-88771 and CVE-2026-88772, had already been exploited as zero-days against unmitigated appliances before any patch existed [1][2]. Both flaws carry a CVSS v4.0 score of 9.5: CVE-2026-88771 is an improper input validation defect that lets an unauthenticated attacker run arbitrary commands against every affected deployment in its default configuration, while CVE-2026-88772 is a memory buffer boundary violation reachable when DTLS is enabled, which it is by default on VPN virtual servers [3][4]. CISA added both to its Known Exploited Vulnerabilities catalog on September 27 and, under Binding Operational Directive 26-04, ordered federal civilian agencies to patch or disconnect affected appliances by September 30, 2026 — a compressed timeline consistent with the unauthenticated, pre-authentication severity of both flaws [1][2][9]. Independent researchers reported that exploitation activity had been underway for weeks before public disclosure, with European government cybersecurity authorities privately warning organizations days ahead of Citrix's bulletin, and Citrix itself has cautioned that its published indicators of compromise may fail to identify some actual intrusions [5][6]. This is at least the fourth major NetScaler zero-day event in roughly three years, following the original CitrixBleed session-hijacking flaw and two subsequent "CitrixBleed" variants, a pattern that CSA's prior research has already flagged as a structural risk tied to NetScaler's role as a widely deployed internet-facing trust boundary [7].

Background

NetScaler ADC and NetScaler Gateway, produced by Cloud Software Group's Citrix business unit, are among the most widely deployed application delivery controllers and SSL VPN gateways in enterprise and government networks, routinely sitting at the perimeter where they terminate remote-access sessions and load-balance traffic to internal applications. This position generally makes any NetScaler vulnerability disproportionately consequential: a flaw here does not merely expose a single application but can hand an attacker a foothold inside the authentication boundary itself, with visibility into internal network segments the appliance was deployed to protect. Citrix's own security bulletin CTX697096, published September 27, 2026, disclosed eight distinct CVEs in a single release, ranging from CVSS 7.0 to 9.5, spanning improper input validation, memory overflow, HTTP request smuggling, policy bypass, and TCP sequence prediction weaknesses [3][4]. Six of the eight are memory-overflow or logic defects

that require non-default configurations such as DTLS, Oracle load-balancing setups, or non-HTTP Layer 7 protocol deployments; CVE-2026-88771 stands apart because it affects every NetScaler ADC and Gateway instance running an affected build, with no special feature flag required [3].

Citrix stated in its bulletin that exploitation of CVE-2026-88771 and CVE-2026-88772 had already been observed against unmitigated deployments, and CISA's alert the same day confirmed threat actors were exploiting both "globally" [1][3]. The public disclosure timeline understates how long the activity had actually been underway. Security researcher Kevin Beaumont reported that exploitation had occurred throughout September 2026, and that European government sources had been warning organizations about active attacks for roughly a week before the Friday, September 27 bulletin, with early notice reportedly originating from the Dutch National Cyber Security Centre [5]. No public reporting has attributed the campaign to a specific named threat actor or group as of this writing, and Citrix has not indicated how the vulnerabilities were discovered or by whom [5][6].

This is not an isolated event for the NetScaler product line. The original CitrixBleed flaw, CVE-2023-4966, allowed attackers to lift authenticated session tokens directly from appliance memory and bypass multi-factor authentication entirely, and was exploited by LockBit-affiliated ransomware actors against organizations including Boeing, ICBC, and DP World [7]. A second variant, CVE-2025-5777 ("CitrixBleed 2"), and a third, CVE-2026-3055 ("CitrixBleed 3," CVSS 9.3), repeated the same memory-disclosure pattern through the SAML identity provider code path; CVE-2026-3055 was subsequently added to CISA's KEV catalog, confirming active exploitation, though public reporting on its exploitation volume is limited [8]. CSA's own research note on the fourth CitrixBleed-lineage flaw, CVE-2026-8451, disclosed in June 2026, documented exploitation attempts within roughly 24 hours of that bulletin and warned that the recurrence of critical memory-safety defects in NetScaler's authentication code represented a structural pattern rather than a series of unrelated incidents [7]. Tenable's research places that pattern in broader context: over the past seven years, roughly two-thirds of threat activity targeting NetScaler has involved advanced persistent threat groups, and one-third has involved ransomware operators and their affiliates, with thirteen distinct NetScaler CVEs now listed in CISA's KEV catalog as of this disclosure [6].

Security Analysis

CVE-2026-88771's practical danger lies in its combination of low attack complexity, no authentication requirement, and universal applicability across default NetScaler ADC and Gateway configurations. Improper input validation of this kind typically allows an attacker to smuggle attacker-controlled data into a code path that treats it as a command or executable instruction; watchTowr's independent technical analysis describes attackers exploiting the flaw by injecting malicious content through the

User-Agent and login fields, which the appliance's logging process then parses and interprets as shell commands via metacharacter injection [11]. Because no special feature needs to be enabled, every unpatched, internet-reachable NetScaler ADC or Gateway instance is a viable target regardless of how conservatively it was configured, which is precisely the condition that produces the kind of broad, opportunistic scanning-and-exploitation activity CISA and independent researchers have both described [1][3].

CVE-2026-88772 is narrower in one dimension and broader in another. It requires DTLS to be enabled, but DTLS ships enabled by default on VPN virtual servers, meaning the large population of NetScaler Gateway deployments used for remote-access VPN termination meet the precondition without any deliberate administrator choice [3][4]. Exploiting a memory buffer boundary violation over DTLS, a UDP-based transport, generally demands more attacker sophistication than a straightforward input-validation bug, which analysts have cited as a plausible reason its observed exploitation volume trails CVE-2026-88771's, even though both carry the same 9.5 severity score [4]. The practical effect for defenders is the same regardless of relative sophistication: both vulnerabilities permit remote code execution on a device that mediates authentication for everything behind it, and guidance from Citrix and CISA instructs administrators to treat compromise as the default assumption for any instance that was internet-facing and unpatched during the exploitation window, rather than something to be ruled out through routine review [1][3].

Detection guidance published alongside the disclosure illustrates both the value and limits of after-the-fact forensics on this class of vulnerability. Beaumont's proposed detection logic looks for base64-encoded strings appended directly after the User-Agent header with no separating space, and for the string "pitboss" followed by shell interpolation patterns in NetScaler logs, indicative of a specific webshell family observed in the wild [5]. Citrix has acknowledged, however, that the indicators of compromise it has published may fail to identify actual compromises, and independent researchers have noted that webshell artifacts appear to be unique per compromised device, which complicates signature-based sweeps across a fleet of appliances [1][5]. This gap between disclosure and reliable detection is consistent with the pattern CSA has documented across recent edge-appliance zero-days: patch deployment alone does not evict an attacker who established persistence, session tokens, or a webshell before the patch was applied, and organizations that patch without first checking for compromise risk leaving an existing foothold in place [7].

The following table summarizes the eight disclosed vulnerabilities and their relative severity and exploitation status.

CVE	CVSS v4.0	Type	Precondition	Exploitation Status
CVE-2026-88771	9.5	Improper input validation → unauthenticated RCE	None (default config)	Actively exploited, zero-day
CVE-2026-88772	9.5	Memory overflow → RCE or DoS	DTLS enabled (default on VPN virtual servers)	Actively exploited, zero-day
CVE-2026-88773	9.3	HTTP request smuggling	Varies by deployment	Not reported as exploited
CVE-2026-88775	8.8	Memory overflow	Gateway/AAA virtual server configurations	Not reported as exploited
CVE-2026-88776	8.8	Memory overflow	Oracle load-balancing configurations	Not reported as exploited
CVE-2026-88777	8.8	Memory overflow	Non-HTTP Layer 7 protocol deployments	Not reported as exploited
CVE-2026-88778	8.8	TCP sequence number prediction	TCP configuration enabled	Not reported as exploited
CVE-2026-88774	7.0	Policy bypass via HTTP URL expressions	Specific policy configurations	Not reported as exploited

Sources: [3][4].

Recommendations

Immediate Actions

Organizations running NetScaler ADC or NetScaler Gateway should confirm their build number against the fixed versions Citrix published on September 27, 2026: 14.1-73.37 or later on the 14.1 branch, 13.1-64.23 or later on the 13.1 branch, and the corresponding FIPS and NDcPP builds [1][3]. Versions 12.1 and 13.0 are not listed among the patched branches in Citrix's bulletin [3][4], and organizations still running them should treat this omission as confirmation that no fix is forthcoming and migration to a supported branch is an emergency action, not a scheduled one. Before applying the patch, security teams should capture forensic evidence, including configuration exports, session and authentication logs, and memory or crash-dump artifacts where feasible, because Citrix has explicitly warned that patching can eliminate the forensic visibility needed to determine whether a given appliance was already compromised [1]. Any instance that was internet-facing and running an affected build during September 2026 should be assumed compromised until an investigation proves otherwise, given researcher reports that exploitation was underway for weeks before public disclosure [5].

Short-Term Mitigations

Following a confirmed or suspected compromise, organizations should isolate the affected appliance from the network, rotate all credentials and API keys stored on or accessible from it, revoke and reissue session tokens, and replace SSL certificates that were present on the device, since an attacker with code execution on the appliance can extract private key material [4]. Rebuilding from a known-good firmware image, rather than relying solely on the vendor patch, is warranted for any instance with confirmed indicators of compromise, since the vendor patch alone does not evict an attacker who has already established persistence on a compromised device. Security teams should hunt for the published indicators, including anomalous base64-encoded content appended to the User-Agent header and log entries referencing "pitboss" alongside shell interpolation syntax, while recognizing that Citrix has cautioned these indicators are not exhaustive and a clean scan does not guarantee a clean device [1][5]. Vulnerability management teams should also verify remediation of the six lower-profile CVEs in the same bulletin, since patch prioritization efforts driven by media coverage of the two zero-days can leave configuration-specific but still critical flaws unaddressed.

Strategic Considerations

This is the fourth significant NetScaler zero-day event since the original CitrixBleed disclosure in 2023, and the recurrence of critical, pre-authentication remote code execution and memory-disclosure defects in the same product line points to a structural risk rather than a series of independent incidents. Organizations with a long-term dependency on NetScaler as a perimeter authentication chokepoint should treat this recurrence as justification for compressing patch SLAs for internet-facing appliances well below general enterprise patch cycles, and for building dedicated vulnerability-operations capacity capable of responding to zero-day disclosures within hours rather than the standard change-management cadence. Longer term, CSA's prior analysis of this vulnerability lineage has recommended migrating remote-access architectures toward Zero Trust Network Access models that reduce reliance on a single perimeter appliance as the sole authentication boundary, since doing so limits the blast radius of any individual device compromise regardless of which vendor or product is affected [7].

CSA Resource Alignment

This event extends a vulnerability lineage CSA has already analyzed directly. CSA's research note, CitrixBleed Infinity: NetScaler Flaw Exploited Within Hours, examined CVE-2026-8451, the fourth prior CitrixBleed-lineage flaw, and documented the same pattern seen again here: a pre-authentication memory-safety defect in NetScaler's authentication-facing code, exploited within hours of disclosure. That note's recommendations, including compressing patch SLAs for edge appliances, building dedicated vulnerability-operations capability, and migrating toward Zero Trust Network Access to reduce reliance on any single perimeter device, apply directly to the current disclosure and reinforce that this is a recurring structural issue rather than an isolated event.

The broader dynamics behind this incident, specifically the collapsing gap between vulnerability disclosure and active exploitation, are addressed in CSA's whitepaper The Bugpocalypse Threshold, which documents that exploitation windows for critical vulnerabilities have compressed to a matter of days industry-wide and that a substantial share of critical vulnerabilities remain unpatched at any given time because remediation capacity has not scaled with disclosure volume. The NetScaler case illustrates that dynamic concretely: exploitation reportedly began before public disclosure, leaving organizations no patch-available window at all in which to act.

Finally, the governance and control-mapping questions this incident raises for vulnerability and threat management programs are addressed by CSA's AI Controls Matrix (AICM) v1.1 [10], whose Threat and Vulnerability Management and Application and Interface Security domains provide a baseline against

which organizations can benchmark their emergency patch response, forensic evidence preservation, and post-compromise credential rotation practices for internet-facing infrastructure of exactly this kind.

References

[1] Cybersecurity and Infrastructure Security Agency. "Critical Zero-Day Vulnerabilities Exploited in Citrix NetScaler ADC, Gateway." CISA, September 27, 2026.

[2] The Hacker News. "CISA Says Attackers Are Exploiting Two Critical Citrix NetScaler Flaws Globally." The Hacker News, September 2026.

[3] Citrix / Cloud Software Group. "Citrix NetScaler ADC and Citrix NetScaler Gateway Security Bulletin for CVE-2026-88771, CVE-2026-88772, CVE-2026-88773, CVE-2026-88774, CVE-2026-88775, CVE-2026-88776, CVE-2026-88777, and CVE-2026-88778." Citrix Support, September 27, 2026.

[4] Rapid7. "Zero-Day Exploitation of Citrix NetScaler ADC and Gateway (CVE-2026-88771 and CVE-2026-88772)." Rapid7 Blog, September 28, 2026.

[5] Help Net Security. "Citrix NetScaler RCE zero-days exploited globally for weeks (CVE-2026-88771, CVE-2026-88772)." Help Net Security, September 28, 2026.

[6] Tenable. "Frequently Asked Questions About Reported Citrix NetScaler Zero-Day Vulnerabilities." Tenable Blog, September 2026.

[7] Cloud Security Alliance AI Safety Initiative. "CitrixBleed Infinity: NetScaler Flaw Exploited Within Hours." CSA Lab Space, July 4, 2026.

[8] Rapid7. "CVE-2026-3055: Citrix NetScaler ADC and NetScaler Gateway Out-of-Bounds Read." Rapid7 Blog, 2026.

[9] BleepingComputer. "CISA orders feds to patch exploited Citrix flaws by Wednesday." BleepingComputer, September 2026.

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

[11] watchTowr Labs. "Oh Look, The Foot Gun Went Off Again: Citrix NetScaler Pre-Auth Command Injection (CVE-2026-88771)." watchTowr Labs, 2026.

