

# CRITICALSTART® Security Advisory

TLP CLEAR // [CS-SA-26-1001] Citrix NetScaler - Active Exploitation and Critical Vulnerabilities

## Executive Summary

The **CRITICALSTART®** Cyber Research Unit (CRU) is tracking active exploitation of Citrix NetScaler Application Delivery Controller (ADC) and NetScaler Gateway appliances, which sit at the edge of many enterprise networks. Citrix has disclosed ten Common Vulnerabilities and Exposures (CVE) entries in three bulletins since September 27, 2026, and three are listed in the Known Exploited Vulnerabilities (KEV) catalog of the Cybersecurity and Infrastructure Security Agency (CISA): CVE-2026-88771, CVE-2026-88772, and CVE-2026-88779.<sup>[1, 2, 5]</sup> The first two allow remote code execution (RCE) and were exploited before fixes existed. The third is a denial of service (DoS) flaw that CISA says attackers can use to trigger code planted through CVE-2026-88771.<sup>[1, 4, 7]</sup> A tenth flaw, CVE-2026-107406, was disclosed October 8 and affects some builds that fixed the earlier issues. No exploitation of it has been reported.<sup>[3, 15]</sup> Organizations should inventory their appliances, upgrade to builds that address all ten, and check for compromise regardless of patch status.<sup>[3, 7, 11]</sup>

| Exposure (Not Compromise)                              | Window                                                                                                       | Confirmed Impact                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 50,277 potentially vulnerable instances <sup>[8]</sup> | Fingerprinting dating back to August 21 (Unit 42). <sup>[8]</sup> CVE-2026-88771 seen September 5 (eSentire) | Rapid7 identified two organizations compromised through CVE-2026-88771. <sup>[9]</sup> Mandiant and Google Threat Intelligence Group (GTIG) described activity affecting organizations in government, financial services, technology, education, and legal and professional services in North America and Europe. <sup>[7]</sup> |

## Background

NetScaler ADC and Gateway appliances provide load balancing, authentication, and remote access for many organizations, so a flaw in them can expose both the appliance and the networks behind it.<sup>[15]</sup> Publications of NetScaler zero-days began circulating on September 26, and Citrix published bulletin CTX697096 the next day. It covered eight vulnerabilities, including CVE-2026-88771, an unauthenticated command injection, and CVE-2026-88772, a memory overflow in the Datagram Transport Layer Security (DTLS) service. Both are scored 9.5 on the Common Vulnerability Scoring System (CVSS) v4.0.<sup>[1, 11]</sup> Citrix reported that both were already being exploited.<sup>[1]</sup> Customers worldwide were warned to disconnect appliances before fixes existed, and multiple hospitals did so, briefly losing patient-portal access.<sup>[15]</sup>

On October 2, administrators reported crashes and reboots on appliances that already carried the September fixes. Citrix confirmed a separate flaw and published CTX697174 on October 3 for CVE-2026-88779, a memory overflow in Security Assertion Markup Language (SAML) processing. It affects appliances configured as a SAML service provider (SP) or identity provider (IdP), and Citrix rates it a DoS flaw (CVSS 8.7).<sup>[2, 13, 14]</sup> CISA added it to KEV on October 4.

In a revision on October 9, CISA described how attackers may use it to force reboots that run code planted through CVE-2026-88771.<sup>[4, 5]</sup> Reports of suspicious activity on patched appliances raised questions about a broader impact, but the evidence cited here does not establish RCE through CVE-2026-88779 itself.<sup>[12, 13, 14]</sup>

On October 8, Citrix disclosed CVE-2026-107406 (CVSS 9.5), a SAML memory overflow that can lead to RCE or DoS. It applies to some builds that fixed the earlier flaws, so earlier patch plans need rechecking. Citrix said it was not aware of unmitigated exploits. [3, 15] Researchers have documented web shells, tunneling tools, and credential theft on compromised appliances, which supports a thorough compromise assessment. That does not mean every exposed appliance was compromised. watchTowr reported that most attempts on its sensors were simple callbacks that tested whether the bug worked. [7, 9, 11]

## Vulnerability Context

### Summary Table

| CVE             | CVSS v4.0 | Description                                              | Prerequisite                                                                                                   | In KEV |
|-----------------|-----------|----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|--------|
| CVE-2026-88771  | 9.5       | Improper input validation leading to unauthenticated RCE | Affected deployment; no additional feature required                                                            | Yes    |
| CVE-2026-88772  | 9.5       | Memory overflow leading to RCE or DoS                    | DTLS enabled                                                                                                   | Yes    |
| CVE-2026-88773  | 9.3       | HTTP request smuggling                                   | HTTP or SSL virtual servers of several types                                                                   | No     |
| CVE-2026-88774  | 7.0       | Feature policy bypass involving HTTP URL expressions     | Policy expressions using HTTP URLs                                                                             | No     |
| CVE-2026-88775  | 8.8       | Memory overflow leading to DoS                           | Gateway or authentication, authorization, and auditing (AAA) virtual server                                    | No     |
| CVE-2026-88776  | 8.8       | Memory overflow leading to DoS                           | Load balancing virtual server of type ORACLE                                                                   | No     |
| CVE-2026-88777  | 8.8       | Memory overflow leading to DoS                           | Applicable non-HTTP layer 7 or network translation feature                                                     | No     |
| CVE-2026-88778  | 8.8       | TCP Initial Sequence Number prediction                   | TCP virtual servers with Enhanced ISN Generation disabled; needs a configuration change as well as the upgrade | No     |
| CVE-2026-88779  | 8.7       | SAML memory overflow leading to DoS                      | SAML SP or IdP configured                                                                                      | Yes    |
| CVE-2026-107406 | 9.5       | SAML memory overflow leading to RCE or DoS               | SAML SP or IdP, depending on build                                                                             | No     |

### CVE-2026-88771: Log Poisoning to Command Execution

CVE-2026-88771 is an unauthenticated command-injection vulnerability that can allow remote attackers to execute arbitrary commands. Citrix assigns it a CVSS v4.0 score of 9.5 and lists no additional feature prerequisite beyond an affected deployment<sup>[1]</sup>. watchTowr's analysis describes how an attacker can submit a request containing attacker-controlled text that NetScaler writes into a log file. A scheduled maintenance script, `ns_monupload_err.pl`, can later pass that text to a shell.<sup>[10]</sup> Because the request and the command execution are separated in time, and the script can take up to 24 hours to run, exploitation may not produce immediate visible activity.<sup>[10, 11]</sup>

Researchers also noted that only the last matching log entry runs, so competing attackers were racing one another. A crash of the packet engine or the SAML service can trigger a warm reload that runs the last injected entry immediately.<sup>[11]</sup>

Researchers reported payloads that create web shells, edit web-server configuration, change file permissions, and collect configuration data.<sup>[8, 9]</sup> Rapid7 described a payload that archives `/flash/nsconfig` into a web-accessible location, which could expose the configuration, encrypted credentials, and TLS (Transport Layer Security) private keys.<sup>[9]</sup>

### CVE-2026-88772: DTLS Memory Corruption

CVE-2026-88772 is a memory-overflow vulnerability in the Datagram Transport Layer Security (DTLS) implementation. Citrix assigns it a CVSS v4.0 score of 9.5 and identifies RCE or DoS as potential impacts. The vulnerability requires DTLS to be enabled, which is the default on Gateway virtual servers unless explicitly disabled<sup>[1]</sup>. Mandiant and GTIG assessed, from frontline telemetry rather than recovered exploit code, that malformed DTLS records sent over User Datagram Protocol (UDP) port 443 corrupt memory in the NetScaler Packet Processing Engine (NSPPE) and give root access.<sup>[7]</sup> watchTowr's analysis describes overflowing a fixed-size reassembly buffer to gain code execution.<sup>[11]</sup>

Mandiant and GTIG reported two log patterns they associate with successful exploitation: a DTLS handshake failure with an internal-error reason, and an NSPPE exit followed by a `pitboss ... NOT restarting NSPPE` message.<sup>[7]</sup> A handshake failure or crash alone does not prove successful exploitation. The surrounding sequence of events matters.

### Post-Exploitation Activity

Mandiant and GTIG reported WHIPSHOT, a PHP (Hypertext Preprocessor) web shell that hides encoded command-and-control (C2) traffic in Hypertext Transfer Protocol (HTTP) headers, and SLAPSHOT, a Python tunneler that proxies traffic into internal networks. Their reporting describes reconnaissance and credential theft in at least one intrusion.<sup>[7]</sup>

watchTowr's sensor network captured a wider range of activity, including a Sliver C2 implant, a trojanized SSH server, a Perl installer that adds an administrator account and a password-protected web shell, and an operator who sprayed SSH keys and web shells and swept for credentials and API keys. Some of this activity failed. The Perl installer's web shell did not work under default settings, because the packet engine strips the cookie it needs.<sup>[11]</sup> Other responders reported the Platypus remote-access tool, and Binary Defense found that web shell directories do not synchronize to the high availability (HA) secondary node, so both nodes need separate triage.<sup>[17]</sup> A reported filename or network indicator should prompt investigation, not automatically establish compromise or attribution. Conversely, the absence of a known indicator does not show that an appliance is clean.

### CVE-2026-88779: SAML Memory Overflow and Denial of Service

CVE-2026-88779 affects NetScaler ADC and Gateway appliances configured as a SAML service provider or identity provider. Citrix assigns the vulnerability a CVSS v4.0 score of 8.7 and identifies denial of service as its documented impact. Repeated triggering may cause sustained disruption. Administrators can inspect configuration for the following entries:

- `add authentication samlAction`
- `add authentication samlIdPProfile`

These entries indicate SAML configuration and should be evaluated against the appliance's version and the conditions in CTX697174. <sup>[2]</sup> watchTowr reproduced the crash behavior and described the vulnerability as a denial-of-service issue. Separate reporting described suspicious activity on patched appliances, including a possible binary download and one administrator logged crafted SAML usernames that fetch a payload from `213.209.159[.]55` shortly before crashes. The reports warrant investigation, but the evidence cited here does not conclusively establish RCE through CVE-2026-88779. <sup>[13]</sup>

CRU recommends reviewing SAML-enabled appliances that experienced unexplained crashes, reboots, unusual downloads, or suspicious outbound connections during the relevant period. Correlate appliance logs, network telemetry, process activity, file changes, and evidence from both high-availability nodes.

### CVE-2026-107406: Additional Critical SAML Vulnerability

CVE-2026-107406 is a separate memory-overflow vulnerability disclosed on October 8. Citrix assigns it a CVSS v4.0 score of 9.5 and identifies potential RCE or DoS. For applicability, the appliance must be configured as a SAML SP or IdP, and the role depends on the build.<sup>[3]</sup>

- On 14.1-73.37 to 14.1-73.41, 13.1-64.23 to 13.1-64.28, and the matching FIPS and NDcPP builds, the flaw applies only when the appliance is a SAML IdP.<sup>[3]</sup>
- On builds before 14.1-73.37 or 13.1-64.23 (and the matching FIPS and NDcPP builds), it applies when the appliance is either a SAML SP or IdP.<sup>[3]</sup>

Finding a SAML entry in the configuration is not enough on its own. Administrators need to match the entry against the version range in CTX697191.<sup>[3, 16]</sup> The bulletin lists no workaround, and removing unused SAML configurations reduces exposure but does not fix the flaw.<sup>[3, 17]</sup> The disclosure alone does not show that any appliance was exploited. Rapid7's Stephen Fewer noted that memory-corruption bugs are generally harder to exploit at scale than CVE-2026-88771, and no successful exploitation had been publicly reported.<sup>[15]</sup>

## MITRE ATT&CK Mapping

The mapping below, drawn from the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework, describes behaviors that researchers observed or reported. Which techniques apply to a given intrusion depends on what an investigation establishes.

| ATT&CK ID | Technique                                                      | Relevance to this campaign                                                                                                              |
|-----------|----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| T1595.002 | Active Scanning: Vulnerability Scanning                        | Fingerprinting of exposed NetScaler appliances <sup>[8, 11]</sup>                                                                       |
| T1190     | Exploit Public-Facing Application                              | CVE-2026-88771 and CVE-2026-88772. CVE-2026-88779 and CVE-2026-107406 should be assessed on the evidence for each. <sup>[1, 2, 3]</sup> |
| T1059.004 | Command and Scripting Interpreter: Unix Shell                  | Commands run through the log-poisoning path <sup>[10]</sup>                                                                             |
| T1505.003 | Server Software Component: Web Shell                           | Reported PHP web shells and staged payloads <sup>[7, 8, 11]</sup>                                                                       |
| T1548.001 | Abuse Elevation Control Mechanism: Setuid and Setgid           | Reported setuid changes on <code>/bin/sh</code> <sup>[7, 8]</sup>                                                                       |
| T1132.001 | Data Encoding: Standard Encoding                               | Base64-encoded commands and C2 traffic in headers <sup>[7]</sup>                                                                        |
| T1090     | Proxy                                                          | SLAPSHOT tunneling into internal networks <sup>[7]</sup>                                                                                |
| T1005     | Data from Local System                                         | Reported collection of appliance configuration data <sup>[9, 11]</sup>                                                                  |
| T1499.004 | Endpoint Denial of Service: Application or System Exploitation | SAML-related crashes and forced reboots <sup>[4, 9]</sup>                                                                               |

## Implications for Organizations

NetScaler appliances can hold configuration data, authentication secrets, certificates, and private keys, and a compromised appliance can give an attacker a path into internal networks. Researchers have documented web shells, tunneling tools, and credential-theft activity in this campaign.<sup>[7, 9, 11]</sup>

Patching and compromise assessment are separate workstreams. An appliance may be patched yet still contain persistence artifacts, and an exposed appliance is not necessarily compromised. watchTowr advises that internet-facing appliances that were unpatched should be treated as potentially compromised, and that patched appliances should still be reviewed for earlier exploitation.<sup>[11]</sup>

If compromise is confirmed or strongly suspected, the response should extend beyond the appliance to identity infrastructure, directory services, certificates, and systems reachable through the Gateway. Credential rotation and rebuilding should be coordinated so that stolen secrets cannot be reused.<sup>[7, 9]</sup> Because Citrix issued three bulletins in under two weeks, organizations may also prefer to move directly to the current target build instead of upgrading in steps.<sup>[1, 2, 3]</sup>

## Prioritized Mitigation Strategies

To improve your organization's security posture considering the Citrix NetScaler exploitation, CRU recommends the following:

### Immediate (Within 24 hours)

- **Inventory all customer-managed NetScaler instances.** Include internet-facing systems, internal instances, test and disaster-recovery systems, both HA nodes, and Secure Private Access hybrid deployments. Record exact builds and editions.<sup>[1, 2, 3]</sup>
- **Check applicability against all three bulletins.** Record SAML role, DTLS status, and relevant TCP settings for each appliance.<sup>[1, 2, 3]</sup>
- **Preserve evidence before rebooting or upgrading when compromise is suspected.** Collect logs, technical support bundles, remote syslog records, network telemetry, and memory or virtual machine snapshots where feasible. watchTowr notes that running processes and memory-resident implants are lost on restart.<sup>[7, 11]</sup>
- **Upgrade to an appropriate current fixed release.** Choose a build that addresses every applicable vulnerability, including CVE-2026-107406, and do not rely only on the original matrix.<sup>[3]</sup>
- **Use interim mitigations only where supported.** For CVE-2026-88772, blocking inbound UDP/443 upstream or disabling DTLS on affected Gateway virtual servers may reduce exposure where appropriate, but this does not address CVE-2026-88771. For CVE-2026-88779, Citrix offers Global Deny List signatures through NetScaler Console on specific intermediate builds. For SAML issues, use only mitigations that Citrix documents for the release and configuration.<sup>[7, 12]</sup>
- **Restrict outbound connectivity.** Investigate unexpected outbound traffic from NetScaler appliances and apply egress controls that fit operational needs. Treat the indicator table below as an aid to investigation, not a complete blocklist.<sup>[7]</sup>
- **Run available detection tooling.** Use the latest Citrix-recommended indicator of compromise (IOC) scan. A clean result is one piece of evidence, not proof, and the latest script can report a false positive for nobody processes.<sup>[12, 17]</sup>

## Short Term

- **Hunt on both HA nodes.** Look for unexpected `httpd.conf` handlers or aliases, suspicious PHP files, unexplained `setuid` changes, unusual scheduled tasks, `pitboss` log entries containing shell characters, DTLS handshake failures followed by NSPPE exits, and unexpected authentication-service crashes. Compare findings with current vendor and researcher indicators.<sup>[7, 8, 10, 17]</sup>
- **Investigate SAML-related crashes and downloads.** Correlate service failures, reboots, unexpected binaries, file changes, and outbound connections. A crash alone does not establish RCE but correlated suspicious activity merits forensic review even though the vendor describes the flaw as DoS.<sup>[4, 13]</sup>
- **Rebuild compromised appliances.** Isolate affected systems as appropriate, control HA synchronization, deploy a trusted image at a fixed release, and migrate only a reviewed configuration.<sup>[7, 17]</sup>
- **Rotate potentially exposed secrets.** Prioritize administrator credentials, LDAP (Lightweight Directory Access Protocol) bind credentials, RADIUS (Remote Authentication Dial-In User Service) and TACACS (Terminal Access Controller Access-Control System) secrets, SNMP (Simple Network Management Protocol) credentials, certificates, and private keys, and coordinate with dependent services.<sup>[7, 9, 11]</sup>
- **Review downstream systems** for lateral movement, unauthorized authentication, or credential misuse.<sup>[7, 9]</sup>
- **Review Enhanced ISN Generation.** For CVE-2026-88778, apply the configuration change Citrix prescribes. An upgrade alone may not satisfy it.<sup>[1]</sup>
- **Centralize logging.** Forward system, application, authentication, and network events to a security information and event management (SIEM) platform and keep enough history for retrospective investigation.<sup>[17]</sup>

## Conclusion

Citrix reported exploitation of CVE-2026-88771 and CVE-2026-88772, which were exploited before fixes existed. A third flaw, CVE-2026-88779, was added to KEV and is documented by Citrix as a SAML denial-of-service issue. CISA describes how it can be used to force reboots that trigger code planted through CVE-2026-88771 on unpatched appliances, and RCE through the flaw itself is not established by the evidence cited here.<sup>[2, 4, 5]</sup> Citrix then disclosed CVE-2026-107406, a critical SAML memory overflow with potential RCE or DoS impact that affects some builds that fixed the earlier flaws. Organizations need to account for it when checking patch status and SAML configuration.<sup>[3]</sup>

The recommended response is to inventory affected instances, confirm each vulnerability's prerequisites, upgrade to an appropriate fixed release, investigate for compromise, preserve evidence where needed, and rotate secrets that may have been exposed. A successful upgrade is essential, but it does not show that an appliance is free of persistence or that downstream systems are unaffected.<sup>[3, 7, 9, 11]</sup>

For more threat reports, including H2 2025 detailing trending cybersecurity concerns visit [Critical Start's Intel Hub](#). Should anything new surface, this advisory will be updated. This advisory was written using the best intelligence available at the time and is subject to change as additional information becomes available.

## What Critical Start is Doing

CRU continues to actively monitor the Citrix NetScaler exploit campaign and work closely with the SOC for heightened vigilance and Security Engineering team to implement any relevant detections. For future updates, CRU will post updates via Cyber Operations Risk & Response™ Bulletins and on the [CRITICALSTART® Intelligence Hub](#).

## Further Reading

- [1] Citrix (September 27, 2026). NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2026-88771 through CVE-2026-88778 (CTX697096). <https://support.citrix.com/external/article/CTX697096/citrix-netscaler-adc-and-citrix-netscale.html>
- [2] Citrix (October 3, 2026). NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2026-88779 (CTX697174). <https://support.citrix.com/external/article/CTX697174/citrix-netscaler-adc-and-citrix-netscale.html>
- [3] Citrix (October 8, 2026). NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2026-107406 (CTX697191). <https://support.citrix.com/external/article/CTX697191/citrix-netscaler-adc-and-citrix-netscale.html>
- [4] CISA (September 27, 2026; revised October 9, 2026). Critical Zero-Day Vulnerabilities Exploited in Citrix NetScaler ADC, Gateway. Read through search-result excerpts of the revision note, because the page blocked direct retrieval. <https://www.cisa.gov/news-events/alerts/2026/09/27/critical-zero-day-vulnerabilities-exploited-citrix-netscaler-adc-gateway>
- [5] CISA (October 4, 2026). CISA Adds One Known Exploited Vulnerability to Catalog. <https://www.cisa.gov/news-events/alerts/2026/10/04/cisa-adds-one-known-exploited-vulnerability-catalog>
- [6] CISA. Known Exploited Vulnerabilities Catalog. Check here for the current listing status of each CVE. <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- [7] Mandiant and Google Threat Intelligence Group (September 29, 2026). Defending Against Active Exploitation of Citrix NetScaler ADC and Gateway Appliances. <https://cloud.google.com/blog/topics/threat-intelligence/defending-against-active-exploitation-of-citrix-netscaler-adc-and-gateway-appliances/>
- [8] Unit 42, Palo Alto Networks (September 30, 2026; updated October 1, 2026). Threat Brief: NetScaler Zero Days CVE-2026-88771 and CVE-2026-88772 Exploited in the Wild. <https://unit42.paloaltonetworks.com/netscaler-zero-days-exploited/>
- [9] Rapid7 (September 28, 2026; updated October 5, 2026). Zero-Day Exploitation of Citrix NetScaler ADC and Gateway: CVE-2026-88771 and CVE-2026-88772. <https://www.rapid7.com/blog/post/etr-zero-day-exploitation-of-citrix-netscaler-adc-and-gateway-cve-2026-88771-and-cve-2026-88772/>
- [10] watchTowr Labs (September 28, 2026). Oh Look, The Foot Gun Went Off Again (Citrix NetScaler PreAuth Command Injection CVE-2026-88771). <https://labs.watchtower.com/oh-look-the-foot-gun-went-off-again-citrix-netscaler-preauth-command-injection-cve-2026-88771/>
- [11] watchTowr Intel (October 7, 2026). Post-Exploitation Analysis and Artifacts: Citrix NetScaler CVE-2026-88771. <https://watchtower.com/intelligence/post-exploitation-analysis-artifacts-citrix-netscaler-cve-2026-88771/>
- [12] watchTowr (October 5, 2026; updated October 6, 2026). Frequently Asked Questions About the Citrix NetScaler Denial Of Service (Memory Overflow) (CVE-2026-88779). <https://watchtower.com/intelligence/citrix-netscaler-cve-2026-88779-faq/>
- [13] L. Abrams, BleepingComputer (October 4, 2026; updated October 5, 2026). Citrix patches NetScaler SAML zero-day exploited in attacks. <https://www.bleepingcomputer.com/news/security/citrix-patches-netscaler-saml-zero-day-exploited-in-attacks/>

[14] E. Kovacs, SecurityWeek (October 5, 2026). Exploitation of Citrix NetScaler Zero-Day Hits Appliances Patched Days Earlier. <https://www.securityweek.com/exploitation-of-citrix-netscaler-zero-day-hits-appliances-patched-days-earlier/>

[15] D. Jones, Cybersecurity Dive (October 12, 2026). CISA calls on Citrix NetScaler customers to patch as new flaws disclosed. <https://www.cybersecuritydive.com/news/cisa-citrix-netscaler-customers-patch-new-flaws-disclosed/832741/>

[16] G. Baran, Cyber Security News (October 9, 2026). Citrix Urges NetScaler ADC and Gateway Customers to Patch for New Critical RCE Vulnerability. Used for build ranges only; its researcher credits differ from the Citrix bulletin. <https://cybersecuritynews.com/citrix-netscaler-adc-and-gateway-rce/>

[17] PitScaler (updated October 14, 2026). CVE-2026-88771: Citrix NetScaler unauthenticated remote code execution. Independent, sourced tracker; secondary. Relays findings from eSentire, Beazley Security, Binary Defense, the Mandiant chief technology officer, the Citrix community blog, the NHS England alert, and the October 14 KEV re-check. <https://pitscaler.com/cve-2026-88771/>

## Appendix

### Indicators of Compromise

The indicators below were reported in research on this campaign. Infrastructure changes, indicators may be shared or reused, and not every victim shows every artifact. Validate each indicator against its original source and observation period before operational use. watchTowr also maintains a public indicator repository.<sup>[7, 8, 11]</sup>

| Type        | Indicator                                                                       | Notes                                                                                                                                                   |
|-------------|---------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| IPv4        | 104.248.244[.]66, 77.83.199[.]39, 193.149.176[.]207, 162.33.178[.]9             | Reported with CVE-2026-88771 and CVE-2026-88772 activity. Unit 42 also listed shared Cloudflare WARP addresses, which are excluded here. <sup>[8]</sup> |
| IPv4        | 143.198.7[.]94, 157.254.167[.]12                                                | Reported scanning, staging, or web shell installation <sup>[7]</sup>                                                                                    |
| IPv4        | 213.209.159[.]55                                                                | Reported as a possible payload host around CVE-2026-88779 activity. The relationship and execution status are not established. <sup>[13]</sup>          |
| Host path   | /var/netcaler/logon/LogonPoint/custom/.ctxs.receive                             | Reported hidden PHP web shell <sup>[8, 11]</sup>                                                                                                        |
| Host path   | /vpn/scripts/linux/nsg64.deb, nsgclient18.deb, nsginstaller*.deb, *.sig         | Reported filenames for staged files; verify contents and provenance <sup>[7, 8]</sup>                                                                   |
| Host path   | /tmp/.uxdport, /tmp/.uxdlock                                                    | Reported SLAPSHOT artifacts <sup>[7]</sup>                                                                                                              |
| Host path   | /vpn/c                                                                          | Reported location of an archive of /flash/nsconfig. If present, assess whether configuration data and secrets were exposed. <sup>[9]</sup>              |
| Log pattern | pitboss entries containing shell metacharacters                                 | May indicate attempts to use the log-processing path; validate the surrounding events <sup>[10, 11]</sup>                                               |
| Log pattern | DTLS handshake failure with an internal-error reason, followed by an NSPPE exit | Investigate as a possible exploitation sequence; a crash alone is not proof <sup>[7]</sup>                                                              |
| SHA-256     | ae22ef2517b5c0fb47f78745b9cb5260acee0e751b89bcd354640ff8bc8d29ec                | Reported hash for an nsg64 .deb web shell. Confirm against the original IOC publication before blocking. <sup>[8]</sup>                                 |

This list is not exhaustive. Researchers reported many payloads and variations, and web shell names and hashes often differ between victims.<sup>[8, 11]</sup>