

Companion to: Emergency Triage and Patch Required: Two Citrix NetScaler Zero-Days Under Global Attack

Reference Bulletin Date: October 02, 2026 | For internal use and client technical response

Commands & Syntax Notice: Commands and code in this document are reproduced from cited sources as a reference only. Results may vary based on your environment, OS version, and tooling. Validate in a test environment before running in production.

IOC Notice: Indicators listed here reflect those reported by cited sources at time of publication and are not exhaustive. Threat actor infrastructure evolves — consult current threat intelligence feeds and your EDR/SIEM for the most complete picture. Absence of these indicators does not confirm a clean environment.

Source labels match the bulletin's References. Where a command or indicator was relayed through the community write-up at Poppelgaard.com rather than read in the original publisher's report, the original publisher is named and the item should be verified against that report before use.

1. PATCH VERIFICATION

1.1 Identify build and compare with fixed versions

- On every NetScaler (both HA nodes, DR, lab, Secure Private Access hybrid instances), record the running build: `show ns version`. Compare to the table below.

Product	Affected	Fixed	Lifecycle
ADC and Gateway 14.1	Before 14.1-73.37	14.1-73.37 and later	Supported (EOL ~2030)
ADC and Gateway 13.1	Before 13.1-64.23	13.1-64.23 and later (use 13.1-64.24 if <code>show ns variable</code> returns output)	End of Maintenance 9/15/26; EOL 9/15/27
ADC 14.1-FIPS	Before 14.1-73.37 FIPS	14.1-73.37 FIPS and later	Unknown
ADC 13.1-FIPS and 13.1-NDcPP	Before 13.1-37.279	13.1-37.279 and later	Unknown
ADC and Gateway 13.0	All builds †	No fix	EOL 7/15/24
ADC and Gateway 12.1	All builds †	No fix	EOL 5/30/23

† EOL/EOS systems cannot receive vendor patches. Immediate isolation or migration is required. Citrix's bulletin lists only supported builds; the "no fix, end of life" status for 12.1 and 13.0 comes from lifecycle data and secondary reporting. (Source: Vendor – Citrix CTX697096 and CTX241500 lifecycle page) Citrix-managed cloud services and Adaptive Authentication are updated by Citrix.

1.2 Pre-upgrade checks

- 13.1 only: run `show ns variable`. If it returns any variables, upgrade to 13.1-64.24, because 13.1-64.23 can enter a cyclic reboot. (Source: Vendor – Citrix guidance, relayed by watchTower and other researchers)
- Confirm your identity provider signs SAML assertions. Unsigned assertions are no longer accepted after the upgrade and are auto-converted to the secure default, which breaks logons for IdPs that do not sign: `grep -i "samlRejectUnsignedAssertion OFF" /nsconfig/ns.conf` (Source: Vendor – Citrix Tech Zone, relayed by Poppelgaard)
- NetScaler Console's Security Advisory scan may falsely flag 13.1-64.23 as vulnerable; Citrix is correcting this through an automatic advisory update. (Source: Vendor – Citrix Tech Zone, relayed by Poppelgaard)

1.3 Check which CVE preconditions your configuration meets

- Run these against `/nsconfig/ns.conf` (or `show ns runningConfig`) on the appliance shell, and in every admin partition. (Source: Vendor – Citrix CTX697096)

CVE	Precondition	How to check
CVE-2026-88771	All deployments, default configuration	No check needed. Every appliance on an affected build is vulnerable.
CVE-2026-88772	DTLS enabled (default on VPN vServers)	Vulnerable if a VPN vServer lacks <code>-dtls OFF</code> (for example <code>add vpn vserver vpn1 SSL 10.0.0.0 443 -Listenpolicy NONE</code>), or any vServer is of type DTLS (<code>add vpn vserver vs1 DTLS 10.11.1.1 443</code>). <code>-dtls OFF</code> means the precondition is not met.
CVE-2026-88773, CVE-2026-88774	HTTP/SSL vServers (88774: any HTTP URL-based policy expression)	<code>grep -iE "^add (lb cs vpn authentication) vserver .* (HTTP SSL)" /nsconfig/ns.conf</code>
CVE-2026-88775	Gateway (SSL VPN, ICA Proxy, CVPN, RDP Proxy) or AAA vServer	<code>grep -iE "^add (vpn authentication) vserver " /nsconfig/ns.conf</code>
CVE-2026-88776	LB vServer of type ORACLE	<code>grep -iE "^add lb vserver.*ORACLE" /nsconfig/ns.conf</code>
CVE-2026-88777	LB/CS or CGNAT-LSN/NAT64 with a non-HTTP L7 feature (FTP, RTSP ALG, DNS64, NAT64)	<code>grep -iE "^add (lb cs) vserver .* FTP ^add service .* FTP ^add lb monitor .* FTP ^add lsn group -ftp DISABLED -rtspalg ENABLED -dns64 ENABLED ^add dns (action policy) 64 ^add nat64" /nsconfig/ns.conf</code> (FTP ALG is on by default for LSN groups unless <code>-ftp DISABLED</code>)
CVE-2026-88778	TCP-based vServer present and Enhanced ISN Generation disabled	<code>show ns tcpparam grep "Enhanced ISN Generation" returning DISABLED, with at least one HTTP, SSL, SSL_BRIDGE, TCP, SSL_TCP, FTP, RDP, ORACLE or other TCP-type vServer.</code>

1.4 Enable Enhanced ISN Generation (CVE-2026-88778)

- The firmware upgrade alone does not fix CVE-2026-88778. Enhanced ISN Generation is a global TCP parameter, off by default. (Source: Vendor – Citrix CTX697096 and NetScaler TCP configuration docs)
- GUI: Configuration > System > Settings > Change TCP parameters > tick Enhanced ISN Generation > OK > save the configuration.
- CLI: `set ns tcpparam -enhancedISNgeneration ENABLED`, then `save ns config -all`. Verify with `show ns tcpparam | grep "Enhanced ISN Generation"` (expect ENABLED). (Source: Vendor docs; commands relayed by Poppelgaard)
- Admin partitions: the setting is partition-specific. Repeat in each partition that has TCP-based vServers:

- show ns partition
- switch ns partition <name> then set ns tcpparam -enhancedISNgeneration ENABLED
- switch ns partition default, set it there too, then save ns config -all
- HA pairs: confirm the secondary node shows the setting enabled after synchronization.

1.5 Verify with Tenable and re-scan

- Run Nessus plugin **350844** against all NetScaler assets: tenable.com/plugins/nessus/350844 (netscaler_adc_gateway_cve-2026-88771.nasl, published 9/27/2026, last updated 9/30/2026). One plugin covers all eight CVEs and flags builds below 13.1-64.23, 14.1-73.37, or 13.1-37.279 for FIPS/NDcPP. (Source: Tenable)
- The plugin is version-based: it confirms the build, not the configuration preconditions or compromise status. Use sections 1.3 and 2 for those. Search other plugins at tenable.com/plugins. (Source: Tenable)
- Note: the plugin's description text pairs the DTLS memory-overflow wording with CVE-2026-88771. Rely on Citrix's bulletin for what each CVE is. (Source: Tenable; Vendor – Citrix CTX697096)
- After upgrading, confirm both HA nodes run the same fixed build, re-run the Citrix IoC scan (section 2.2), and re-scan with plugin 350844.

2. DETECTION / THREAT HUNTING

Scope the hunt back to at least early September 2026: Mandiant places the start of exploitation then, Unit 42 saw fingerprinting from August 21 and web-shell delivery on September 21, and GreyNoise recorded exploitation on September 24. Many appliances keep only about 24 hours of local logs, so a clean log is weak evidence. (Source: Google/Mandiant; Unit 42; GreyNoise)

2.1 Preserve evidence before any upgrade or reboot

- Take a memory-inclusive snapshot (virtual instances) or forensic RAM copy where possible; at least one flaw may leave traces only in memory. (Source: CISA; Google/Mandiant)
- Collect a support bundle (show techsupport) and copy /var/log/*, /var/nslog/* and the Apache/httpd logs off the appliance. (Source: Vendor – Citrix CTX694799; CISA)
- Check /tmp before rebooting: it is emptied at boot and holds some exploit marker files (section 3). (Source: watchTower)

2.2 Run the official Citrix IoC scan

- Requirements: NetScaler Console service, or Console on-premises 14.1-73.36 or later connected through Cloud Connect; instances managed by Console; telemetry channel enabled. (Source: Vendor – Citrix, relayed by Poppelgaard)
- Run: Console > Security Advisory > Indicators of Compromise tab > accept terms > start the scan > download the CSV/PDF per instance. Record scan time, IoC version, appliance build and platform. (Source: Vendor – Citrix)
- Use IoC version 3 or later (v1 Sept 27, v2 Sept 28, v3 Sept 29); re-run if your last scan used an earlier version. No Console upgrade is needed to receive updated IoC content. (Source: Vendor – Citrix Tech Zone, relayed by Poppelgaard)
- Read results carefully: only “No Compromise Detected” is a completed scan; “Skipped” and “Failed to Execute” mean the instance was not checked. A clean result does not prove the appliance was never compromised, and post-patch attack attempts can surface as potential IoCs.
- No Console or telemetry? Open a Citrix Technical Support case citing CTX697096, CVE-2026-88771 and CVE-2026-88772, with a support bundle collected before any upgrade.

2.3 Hunt in logs

- Injected shell commands in authentication log lines (the CVE-2026-88771 technique): (Source: watchTower; CERT-EU; Beazley Security)
 - `zgrep -E 'died NSPPE;|heartbeats.*;|\\$\\{?IFS|pitboss.*;' /var/log/ns.log* /var/log/messages*`
 - Genuine watchdog events also log “missed too many heartbeats”; treat it as an attack only when it appears in an authentication log line or beside shell characters such as `;`, backticks or `${IFS}`. (Source: Beazley Security)
- Two-stage variant: a request to /logon/LogonPoint/tmindex.html carrying a base64 command in the User-Agent after INDEX:, later triggered by a fake logon name. Find and decode: `zgrep -oE 'INDEX:[A-Za-z0-9+/=]{8,}' /var/log/httpaccess* then echo '<value>' | b64decode -r` (Source: CERT-EU)
- Treat sustained requests to /logon/LogonPoint/Authentication/GetUserName as anomalous. (Source: Unit 42)
- The injected text can wait for a background job; a command sent one day can execute the next. An unpatched appliance may still run yesterday's request. (Source: watchTower)

2.4 Hunt on the filesystem and configuration

- Web shells: any PHP in LogonPoint/custom or /var/vpn, whatever the file is named: `grep -rLE '<\\?php|passthru|NSC_TASS' /var/netScaler/logon/LogonPoint/custom /var/vpn` (Source: GreyNoise; Poppelgaard)
- Mandiant reports web shells disguised as client packages, signature files or icons under the Gateway vpn/scripts and vpn/media folders (for example /var/netScaler/gui/vpn/scripts/ and /netScaler/ns_gui/vpn/media/). (Source: Google/Mandiant)
- Web-server config: `grep -Ein "application/x-httpd-php|php_flag|AliasMatch" /etc/httpd.conf`. Any PHP handler for a non-.php extension, or aliases into vpn/media or vpn/scripts, is a red flag. /etc/httpd.conf is rebuilt at boot, so check /nsconfig/httpd.conf too. (Source: Google/Mandiant; GreyNoise)
- Setuid shell: `ls -l /bin/sh` should show no `s` bit; attackers ran `chmod 6555` on it. (Source: GreyNoise; Google/Mandiant)
- Persistence and cleanup: review /nsconfig/rc.netScaler and /nsconfig/nsafter.sh (run at every boot) and cron jobs that delete or empty logs: `ls -la /var/cron/tabs/; crontab -l -u root; crontab -l -u nsroot` (Source: Beazley Security)
- nsmon.pl implant: `ls -la /var/tmp/.nsmon, grep nsmon /etc/crontab /nsconfig/crontab, and sockstat -4l | grep perl` (a listener on a TCP port from 41000 to 41999). (Source: Arctic Wolf)

- Files that prove a command ran (the appliance was exploited even if the payload looks harmless): `nx_verify.html`, `/var/tmp/wtw*`, `/tmp/watchTower`, `c88771.json`. (Source: [Lupovis](#); [watchTower](#); [community](#))
- Config theft: a file such as `/var/netScaler/logon/LogonPoint/xua.html` that is really a tar or gzip archive (file `<path>`). Rapid7 observed an injected command that archives `/flash/nsconfig`. If found, assume `ns.conf` and every private key on the box are stolen. (Source: [Rapid7](#); [Poppelgaard](#))
- HA pairs: run every check on both nodes. HA file sync copied a web shell to the secondary, and it survived a reboot and the upgrade. (Source: [Poppelgaard](#))

2.5 CVE-2026-88772 (DTLS) indicators

- DTLS handshake failures ("Handshake failure-Internal Error") in `ns.log`, packet-engine crashes or restarts (exit with orphan rings, NOT restarting NSPPE), and new files in `/var/core`. (Source: [watchTower](#); [Google/Mandiant](#))
- Tunnel markers: `/tmp/.uxdport`, `/tmp/.uxdlock`, and the string `UXD_IDLE_EXIT`. Unit 42 also observed DTLS exploitation dropping `.deb` web-shell files. (Source: [Google/Mandiant](#); [Unit 42](#))
- Network side: list DTLS sessions to NetScaler addresses in Zeek logs. (Source: [Corelight](#), via [Poppelgaard](#))

2.6 Hunt for credential theft and lateral movement

- Look for `ldapsearch` or `openssl s_client` in `/var/log/sh.log*` and `bash.log*`, PHP or shell scripts under `/netScaler/ns_gui` written after boot, and LDAP/LDAPS or SMB connections from the NetScaler to domain controllers outside normal authentication. If found, rotate the LDAP bind account immediately. (Source: [Kevin Beaumont](#), via [Prophet Security](#) and [Poppelgaard](#))
- Check connections from the NSIP/SNIP to `194[.]26[.]29[.]88` and other listed infrastructure (section 3) in firewall and network logs. (Source: [Corelight](#); [Google/Mandiant](#))
- Detection content: Palo Alto Threat Prevention signature 97562 targets the CVE-2026-88771 command injection. (Source: [Unit 42](#)) Elastic publishes a rule for NetScaler log-poisoning command injection (`initial_access_netScaler_log_poisoning_command_injection`). (Source: [Elastic](#), via [Poppelgaard](#))

3. IOC REFERENCE

IPs and domains are defanged ([.]). Attacker IPs, shell names and file paths differ per victim, so matching nothing here is not proof of a clean appliance. Cloudflare WARP and residential addresses are shared by ordinary users; do not block on them alone.

Type	Indicator	Context	Source
File	<code>/var/netScaler/logon/LogonPoint/custom/.ctxs.receiver</code>	Hidden PHP web shell, unlocked by a <code>CsrfToken</code> cookie; runs the <code>NSC_TASS</code> cookie value	GreyNoise
SHA-256	<code>6f5a2a452a7901323abd21879c6cecccb47c06aeeacbb1b467212f3b11e4b1e7</code>	<code>.ctxs.receiver</code> web shell	GreyNoise
URL path	<code>/logon/LogonPoint/custom/receiver.min.css</code> or <code>receiver.min.<hex>.css</code>	<code>httpd Alias/AliasMatch</code> exposing the web shell	GreyNoise
Request	POST <code>/nf/auth/doAuthentication.do</code> with a login name like <code>pitboss</code> PPE unexpectedly died NSPPE; <code><command>;# X</code>	CVE-2026-88771 exploitation; variants use <code>\${IFS}</code> for spaces	watchTower ; Lupovis
Request	<code>/logon/LogonPoint/tmindex.html</code> with User-Agent <code>INDEX: + base64</code>	Stage 1 of the two-stage injection	CERT-EU
Request	Repeated <code>/logon/LogonPoint/Authentication/GetUserName</code>	Anomalous pre-disclosure activity, Sept 10–27	Unit 42
File	<code>/var/vpn/bookmark/nx_verify.html</code> (canary NX-CVE-OK); <code>/var/tmp/wtw*</code> ; <code>/tmp/watchTower</code>	Proof a command ran	Lupovis ; watchTower
File	<code>/netScaler/ns_gui/vpn/c88771.json</code> ; <code>/var/netScaler/logon/LogonPoint/xua.html</code> (archive)	Config and key theft staging	Rapid7 ; community
Directory	<code>/var/tmp/.nsmon(.cfg,.state)</code> ; cron entry running <code>nsmon.pl</code> every 5 min; Perl listener on TCP 41000–41999	Perl implant <code>nsmon.pl</code>	Arctic Wolf
File / string	<code>/tmp/.uxdport</code> , <code>/tmp/.uxdlock</code> , <code>UXD_IDLE_EXIT</code>	SLAPSHOT tunnel markers	Google/Mandiant
Code	HTTP <code>X_UX</code> or eval on <code>HTTP_NSC_CLIENTTYPE</code> in files under <code>vpn/scripts</code> , <code>vpn/media</code>	WHIPSHOT web shell	Google/Mandiant
Permission	<code>Setuid /bin/sh (chmod 6555)</code>	Post-exploitation privilege setup	GreyNoise; Google/Mandiant
IP	<code>149[.]104[.]78[.]141</code> ; <code>149[.]104[.]78[.]208</code>	Exploitation Sept 24 (GreyNoise); injection attempt Sept 20 (Rapid7)	GreyNoise; Rapid7
IP	<code>77[.]83[.]199[.]39</code> , <code>78[.]47[.]24[.]217</code> , <code>139[.]180[.]152[.]138</code>	Three-stage web-shell dropper, Sept 21	Unit 42
IP	<code>104[.]248[.]244[.]66</code> , <code>137[.]184[.]91[.]207</code>	Earlier fingerprinting (from Aug 21 and Sept 7)	Unit 42
IP	<code>104[.]28[.]247[.]137</code> , <code>193[.]149[.]176[.]207</code>	<code>GetUserName</code> request stream (alongside WARP addresses)	Unit 42
IP	<code>138[.]28[.]234[.]38</code> , <code>82[.]167[.]14[.]7</code> , <code>154[.]217[.]251[.]226</code> , <code>78[.]128[.]113[.]10</code> , <code>85[.]203[.]46[.]191</code>	Live exploitation and scanning captured on decoys	Lupovis
IP	<code>143[.]198[.]7[.]94</code> , <code>157[.]254[.]167[.]12</code>	Campaign infrastructure	Google/Mandiant
IP	<code>194[.]26[.]29[.]88</code>	Reverse-shell host	Corelight

Type	Indicator	Context	Source
Domain	entretiensol[.]com; echvista[.]com; *.instances.httpworkbench[.]com	Payload/C2; DNS exfiltration of command output	Arctic Wolf; PitScaler; Lupovis
User-Agent	ns-88771-poc; PoCbit	Scanners probing CVE-2026-88771 / 88772	Lupovis

A larger community IoC collection (including CSV download) is maintained at pitscaler.com; verify entries against original publishers before blocking.

4. COMPENSATING CONTROLS AND HARDENING

4.1 If you cannot patch immediately

- There is no mitigation for CVE-2026-88771; upgrading is the only fix. Remove Gateway exposure from the internet or restrict it to known source IP ranges until the upgrade is complete. (Source: [watchTower](#); Vendor – Citrix, relayed by [Poppelgaard](#))
- CVE-2026-88772 only: block inbound UDP/443 where DTLS is not needed, or disable DTLS per VPN vServer with `set vpn vserver <name> -dtls OFF`. Users on EDT/UDP fall back to TCP. (Source: [Google/Mandiant](#); [Poppelgaard](#))
- Keep management interfaces off the internet and apply default-deny outbound rules from the NSIP and SNIP. (Source: [Google/Mandiant](#))
- Enable Enhanced ISN Generation now (section 1.4); it is needed regardless. (Source: Vendor – Citrix)

4.2 Logging and monitoring

- Forward `ns.log`, `/var/log/messages` and the HTTP logs to an external SIEM or syslog server; local retention may be only about a day. (Source: Vendor – Citrix; [Google/Mandiant](#))
- Keep firewall logs as well: NAT in front of the Gateway can hide client IPs in appliance logs. (Source: [Poppelgaard](#))
- Enable NetScaler Console File Integrity Monitoring to flag unexpected file changes. (Source: [Poppelgaard](#))

4.3 Response if compromise is suspected or confirmed

- Isolate the appliance from the internet and internal network but keep it powered on until evidence is preserved; do not sync HA from the suspect node. (Source: Vendor – Citrix CTX694799; [Google/Mandiant](#))
- Do not rely on upgrading in place: the update does not remove compromise artifacts. Deploy a new, updated NetScaler instance and migrate the configuration in a controlled, security-reviewed way. (Source: Vendor – Citrix)
- After the upgrade, terminate sessions: `kill icaconnection -all, kill rdp connection -all, kill pcoipConnection -all, kill aaa session -all, clear lb persistentSessions` (Source: [Poppelgaard](#))
- Rotate every secret stored on or passing through the appliance:
 - nsroot and admin accounts
 - LDAP/AD bind accounts, RADIUS secrets, TACACS, SNMP and API credentials, service accounts
 - TLS certificates and private keys (replace the certificates, not only the passwords)
- Also check StoreFront, the Delivery Controllers and the VDAs behind the appliance, and hunt internally for lateral movement from the NSIP/SNIP: new accounts, unusual logons, web shells. (Source: [Google/Mandiant](#); [Poppelgaard](#))

4.4 Unsupported builds

- Do not attempt to patch NetScaler 12.1 (EOL 5/30/23) or 13.0 (EOL 7/15/24). Restrict them from the internet immediately and migrate to 14.1. (Source: Vendor – Citrix lifecycle CTX241500)
- 13.1 receives this fix but has been in End of Maintenance since 9/15/26 and reaches EOL on 9/15/27; plan the 14.1 migration now. (Source: Vendor – Citrix lifecycle CTX241500)