



Executive Summary

This is an emergency-patching week. On September 27, 2026 Citrix published security bulletin CTX697096 confirming that two zero-day vulnerabilities in NetScaler ADC and NetScaler Gateway — CVE-2026-88771 and CVE-2026-88772, both CVSSv4 9.5 — were being actively exploited in the wild. CISA added both to the Known Exploited Vulnerabilities catalog the same day and set a remediation deadline of September 30 for federal civilian agencies: three days, which is short even by KEV standards. CISA stated that threat actors are actively exploiting the vulnerabilities globally. GTI tracks the activity as GLOBAL.26.012 and confirms HEALTHCARE among six targeted industries, with United States and Australia confirmed. The critical operational point is the timeline: GTIG tracked exploitation by multiple distinct threat clusters starting as early as September 9, roughly eighteen days before anyone could patch. Any internet-facing NetScaler appliance that was unpatched during September should be treated as potentially compromised, and patching alone does not resolve that.

The post-exploitation tradecraft reinforces why. Across the clusters GTIG documents PHP web shells disguised as .sig files written into the NetScaler GUI directory structure, Apache configuration modified to enable PHP execution and to rewrite requests for innocuous .ico and .deb resources to the web shell handlers, shell commands appended to NetScaler pitboss process-monitor failure messages so they execute, \${IFS} substitution to defeat whitespace filtering, base64 payloads hidden inside the appliance's own log files, and GREENSNAKE — a Python backdoor using the Google Sheets API for command and control. A separate GTI-tracked cluster, CAMP.26.145, deploys the WHIPSHOT web shell and the SLAPSHOT Python proxy tunnel, sets SUID root on /bin/sh, scrubs its cron entries, and uses regex wiping to strip its own URI paths from Apache access logs while returning spoofed HTTP 404 responses. That is deliberate anti-forensics on the appliance: clean logs are not evidence of a clean appliance.

On the breach side, reporting compiled by Becker's Hospital Review and updated October 1 names 29 health systems reportedly affected by the Oracle Health data breach, including Atrium Health, AdventHealth, Christus Health, ChristianaCare, OSF HealthCare, Baptist Health South Florida, LifeBridge Health and Methodist Le Bonheur Healthcare. A single EHR platform compromise reaching 29 separate provider organizations is the clearest concentration-risk event this series has reported. Set against that, the HIPAA Journal published its H1 2026 breach report on September 30 showing large healthcare breaches DOWN 5.9% year over year and affected individuals down 22.6% — 397 breaches of 500 or more individuals reported to OCR, the lowest H1 total since 2023. Both things are true: fewer breaches, concentrated in larger vendors.

Active Threat Campaigns- Healthcare & Technology

Threat Activity	Type	Key Technique / Detail	Targets	Priority Action
Citrix NetScaler Zero-Days — Multi-Actor Exploitation (GLOBAL.26.012; CVE-2026-88771 and CVE-2026-88772)	Multi-cluster exploitation of edge infrastructure — Espionage (GTI-confirmed)	GTIG tracked exploitation by MULTIPLE threat clusters starting as early as September 9, 2026 — before public disclosure. CVE-2026-88771 is an improper input validation flaw permitting an unauthenticated attacker to execute arbitrary commands, affecting ALL deployments including default configurations. CVE-2026-88772 is a memory corruption flaw in the NetScaler Packet Processing Engine permitting unauthenticated remote code execution via malformed DTLS traffic. Both carry CVSSv4 9.5. Initial access appeared as DTLS handshake failures followed by NSPPE process terminations and appliance kernel re-initialisation. Attackers appended shell commands to	Healthcare GTI-confirmed, among six industries (also Education, Financial Services, Legal & Professional Services, Retail, Telecommunications) — United States and Australia confirmed. CISA states exploitation is occurring globally	CRITICAL — Patch to 14.1-73.37, 13.1-64.23, 14.1-73.37 FIPS or 13.1-37.279 as applicable. The CISA KEV deadline was September 30. Because exploitation preceded disclosure, PATCHING IS NOT SUFFICIENT — hunt for web shells and configuration changes before declaring the appliance clean



Threat Activity	Type	Key Technique / Detail	Targets	Priority Action
		NetScaler pitboss process-monitor failure messages, causing them to execute. Post-exploitation: PHP web shells disguised as .sig files written into the GUI directory structure, Apache configuration modified to enable PHP execution and rewrite requests for innocuous .ico and .deb resources to the web shell handlers, interaction via curl with spoofed Chrome user-agent strings, \${IFS} substitution to bypass whitespace filtering, base64 payloads planted in the appliance's own log files, reverse shells over TCP 443, and GREENSNAKE — a Python backdoor for Linux using the Google Sheets API for command and control		
WHIPSHOT Web Shells and SLAPSHOT Proxy Tunnels (CAMP.26.145 — CVE-2026-88772 zero-day)	Espionage — data theft via edge appliance pivot	A distinct GTI-tracked cluster exploiting the same Citrix zero-day for initial access, then deploying the WHIPSHOT web shell and SLAPSHOT proxy tunneler. The actor modifies httpd.conf to inject AddHandler, php_flag engine on and AliasMatch directives routing /vpn/media/*.ico requests to staged .sig files; sets SUID root permissions on /bin/sh; scrubs /vpn/scripts/linux from /etc/crontab; and uses regex wiping to strip its own URI paths from Apache access logs while returning spoofed HTTP 404 responses. WHIPSHOT bridges traffic to SLAPSHOT, a custom Python SOCKS-like TCP relay, which the actor uses to proxy internal TCP traffic from the NetScaler appliance into the network for reconnaissance and data exfiltration. Activity observed from September 10 to September 27, 2026	GTI-confirmed: Education and Financial Services — United States. Healthcare NOT confirmed for this specific cluster, but it exploits the same appliance and CVE for which Healthcare IS confirmed in GLOBAL.26.012	CRITICAL — The anti-forensic steps matter: this actor edits Apache logs and crontab to erase itself. Absence of evidence in appliance logs is NOT evidence of absence. Check httpd.conf for injected directives and /bin/sh for SUID root
Oracle Health Data Breach — 29 Health Systems Named (reporting updated Oct 1)	Healthcare IT vendor / EHR platform breach	Reporting compiled by Becker's Hospital Review, updated October 1, 2026, lists 29 health systems reportedly affected by the Oracle Health data breach. Named organizations include Albany Med Health System, Huntington Hospital, Christus Health, Munson Healthcare, Atrium Health, Jupiter Medical Center, AdventHealth, Aultman Health System, Lake Regional Health System, OSF HealthCare, Hamilton Medical Center, Methodist Le Bonheur Healthcare, ChristianaCare, North Kansas City Hospital, LifeBridge Health, Glens Falls Hospital, Baptist Health South Florida, Mosaic Life Care, Tallahassee Memorial Healthcare, Union Health, Oaklawn Hospital and Great River Health. The count and the named list are drawn from that compilation rather than from a single vendor disclosure, and individual affected counts are not uniformly published	US health systems using Oracle Health EHR platforms. This is a concentration event: a single vendor compromise reaching 29 separate provider organizations	CRITICAL (if applicable) — If you run Oracle Health or Cerner-lineage platforms, request written confirmation of whether your tenant is in scope and what data categories were involved. Do not wait for individual notification
Microsoft Teams Archive Lures → DLL Search Order Hijacking	Social engineering initial access (motivation not assigned)	GTIG observed an unknown actor gaining initial access primarily through social engineering lures delivered via MICROSOFT TEAMS MESSAGES and web downloads. Victims receive compressed	GTI-confirmed: Legal & Professional Services — United States and United Kingdom. Healthcare	HIGH — Review Microsoft Teams external access and federation settings; most organizations



Threat Activity	Type	Key Technique / Detail	Targets	Priority Action
(CAMP.26.148)		archives — mostly ZIP — containing binaries disguised as Word documents alongside malicious DLLs. On execution a legitimate executable performs DLL search order hijacking to side-load the malicious library directly into memory. In some intrusions the archives also contained vulnerable system drivers to enable low-level access. The actor stages payloads in local directories and runs discovery via WMI, including querying SCREEN REFRESH RATES to assess whether the payload is running in a sandbox or virtual machine. GTIG notes observed post-exploitation activity has been limited and multiple active intrusions remain under investigation. Activity September 1 to 18, 2026	NOT confirmed. Carried because Teams is a primary clinical and administrative collaboration channel and is frequently trusted more than email	harden email far more than Teams. Alert on archives delivered via Teams, on DLL side-loading from user-writable paths, and on WMI display-property queries

Top 4 Priority Actions This Week

1. [CRITICAL] Treat Every September-Exposed NetScaler Appliance as Potentially Compromised

Citrix published bulletin CTX697096 on September 27, 2026 disclosing eight vulnerabilities in NetScaler ADC and NetScaler Gateway, of which CVE-2026-88771 and CVE-2026-88772 are confirmed exploited zero-days carrying CVSSv4 9.5. CVE-2026-88771 is an improper input validation flaw (CWE-20) permitting unauthenticated remote code execution and affecting all deployments including the default configuration — there is no mitigating configuration. CVE-2026-88772 is a memory overflow in the NetScaler Packet Processing Engine (CWE-119) permitting unauthenticated remote code execution via malformed DTLS traffic, and requires the DTLS feature to be enabled; Citrix has indicated attack complexity is high for this one. CISA added both to the KEV catalog on September 27 — the same day as disclosure — and set a remediation deadline of September 30 under its binding operational directive, a three-day window. Fixed builds are 14.1-73.37 and later, 13.1-64.23 and later, 14.1-73.37 FIPS, and 13.1-37.279 for FIPS and NDcPP. Notably, reporting indicates national cyber agencies and IT suppliers were privately contacting Citrix customers and advising them to shut down NetScaler appliances days before patches existed, after NCSC-NL learned of the zero-days from a European partner CERT.

The reason this cannot be closed by patching alone is the exploitation timeline. GTIG tracked exploitation by multiple distinct threat clusters from as early as September 9, and separate reporting places exploitation of CVE-2026-88772 earlier still. That means an appliance patched on September 28 may have been compromised for two to three weeks beforehand, and the documented post-exploitation activity is specifically designed to survive and to hide. Web shells are written as .sig files inside the GUI directory structure where they look like legitimate signature files. Apache configuration is modified so that requests for ordinary-looking .ico and .deb resources are rewritten to the web shell handlers. One cluster strips its own URI paths from Apache access logs using regex wiping and returns spoofed HTTP 404 responses, scrubs its entries from /etc/crontab, and sets SUID root on /bin/sh for later privilege escalation. A clean-looking log is consistent with a compromised appliance.

- Patch immediately to the fixed builds listed above if you have not already; for healthcare organizations the KEV deadline is not binding but should be treated as the benchmark, since NetScaler commonly fronts clinical remote access and VDI
- Hunt before declaring clean: inspect httpd.conf for injected AddHandler, php_flag engine on and AliasMatch directives; look for .sig files in the GUI directory structure; check whether /bin/sh carries SUID root permissions; and review /etc/crontab for removed or altered entries



- Review appliance logs for DTLS handshake failures followed by NSPPE process terminations and kernel re-initialisation events — the documented initial-access signature — and treat gaps or inconsistencies in Apache access logs as suspicious in themselves
- Hunt at the network layer rather than trusting the appliance: look for outbound connections to the Google Sheets API from NetScaler management interfaces (the GREENSNAKE C2 channel), reverse shells over TCP 443, and curl user-agent strings spoofing Google Chrome
- Ingest the 48 GTI indicators from GLOBAL.26.012 and the 5 from CAMP.26.145 — 19 and 4 IP addresses respectively, which is unusually IP-heavy and well suited to firewall and netflow hunting
- If compromise is confirmed or suspected, rotate all credentials and certificates handled by the appliance, including VPN, LDAP bind and SAML signing material, and assume internal reconnaissance occurred — SLAPSHOT exists specifically to proxy traffic from the appliance into the internal network

2. [CRITICAL] Determine Oracle Health Exposure Without Waiting for Notification

Reporting compiled by Becker's Hospital Review and updated October 1, 2026 names 29 health systems reportedly affected by the Oracle Health data breach. The named organizations span large multi-state systems and community hospitals alike, including Albany Med Health System, Huntington Hospital, Christus Health, Munson Healthcare, Atrium Health, Jupiter Medical Center, AdventHealth, Aultman Health System, Lake Regional Health System, OSF HealthCare, Hamilton Medical Center, Methodist Le Bonheur Healthcare, ChristianaCare, North Kansas City Hospital, LifeBridge Health, Glens Falls Hospital, Baptist Health South Florida, Mosaic Life Care, Tallahassee Memorial Healthcare, Union Health, Oaklawn Hospital and Great River Health. Two sourcing caveats are worth stating plainly to leadership. The count and the named list come from a journalistic compilation rather than from a single consolidated vendor disclosure, and per-organization affected counts are not uniformly published. This brief therefore reports the list as reported and does not assert a total number of individuals.

The structural lesson stands regardless of the final figures. An electronic health record platform holds the most sensitive data a provider organization possesses, and a compromise at the platform level reaches every tenant at once. This is the same concentration pattern seen earlier in this series with Conduent, Aesto Health and Craneware, but applied to the clinical system of record rather than a billing or back-office function.

- If you run Oracle Health or Cerner-lineage platforms, request written confirmation now of whether your tenant is in scope, what data categories were involved, and what the notification timeline is — do not wait for individual notification
- Ask specifically about credential and integration exposure, not only patient data: EHR platforms hold interface credentials to laboratory, imaging, pharmacy and billing systems, the same architectural concern raised by the Mirth Connect advisory still open in the tracker
- Review and rotate any credentials your organization supplied to the vendor for integrations, and check federated authentication trust relationships
- Record this as a Business Associate event with the reported facts, the sourcing caveat and the open questions clearly separated, and diary follow-up against the HHS OCR breach portal for confirmed individual counts

3. [HIGH] Close the Microsoft Teams Trust Gap (CAMP.26.148)

GTIG released CAMP.26.148 on October 2, documenting an unknown threat actor gaining initial access primarily through social engineering lures delivered via Microsoft Teams messages and web downloads. Victims receive compressed archives, mostly ZIP files, containing binaries disguised as Word documents alongside malicious DLLs. When the disguised binary runs, a legitimate executable performs DLL search order hijacking to side-load the malicious library directly into memory. In some intrusions the archives also contained vulnerable system drivers to facilitate low-



level access. Post-execution the actor stages payloads locally and runs discovery through Windows Management Instrumentation — including, notably, querying screen refresh rates to judge whether the payload is executing in a sandbox or virtual machine, a sandbox-evasion technique using ordinary hardware telemetry rather than the usual artefact checks. GTIG states that observed post-exploitation activity has been limited so far and that multiple active intrusions remain under investigation. Targeting is GTI-confirmed for Legal & Professional Services in the United States and United Kingdom; healthcare is not confirmed. It is carried here because Teams is a primary clinical and administrative collaboration channel, and because most organizations have invested far more in email security than in Teams external access controls — which is precisely the gap this actor is using.

- Review Microsoft Teams external access and federation settings: restrict who outside your tenant can initiate chats, and consider blocking federation with consumer Microsoft accounts where there is no business need
- Extend attachment controls to Teams: if ZIP files from external senders are blocked in email, confirm the same policy applies to files delivered through Teams
- Alert on DLL side-loading where a legitimate signed executable loads an unsigned library from a user-writable directory such as a recently extracted archive path
- Alert on WMI queries for display properties including refresh rate from non-administrative processes — there is almost no legitimate reason for a document-handling process to inspect monitor hardware
- Brief staff that an archive arriving over Teams from an external party carries the same risk as an email attachment, and that a Word icon does not mean a Word document

4. [HIGH] Use the Quiet Advisory Week to Close the Open Medical Device Actions

The advisory review for this window surfaced no new CISA medical advisory, which leaves the two from September 10 outstanding for a third consecutive reporting cycle. ICSMA-26-253-01 covers three vulnerabilities in NextGen Healthcare Mirth Connect versions 4.7.1 and earlier; the CVE record for CVE-2026-82583 states that an authenticated user can execute arbitrary SQL through a Database Connector API, which could result in disclosure of stored credentials for connected systems, arbitrary file write and denial of service, while CVE-2026-82578 requires no privileges at all. ICSMA-26-253-02 covers CVE-2026-87020 in Orthanc DICOM Server versions earlier than 1.13.0. Both have vendor fixes. There is a direct thematic link to this week's lead item worth drawing out: the Citrix compromises and the Mirth Connect vulnerability are the same class of problem — an infrastructure component that brokers access or credentials for many downstream systems, where compromising the broker yields far more than the component itself. Edge appliances and integration engines deserve the same treatment in your asset criticality model.

- Confirm Mirth Connect is at v4.7.2 or later everywhere it runs, and complete the downstream credential rotation — third week of asking, and it remains the step that determines whether patching actually closed the exposure
- Confirm Orthanc instances are at 1.13.0 or later, including research and teaching deployments outside IT procurement
- Review your asset criticality model to ensure edge appliances (NetScaler, VPN concentrators, reverse proxies) and integration engines (Mirth and equivalents) are rated on what they broker access to, not on the data they store themselves
- For the unpatchable items — GDCM at week 28, pydicom/pynetdicom, and the Pulsetto stimulator — confirm compensating controls are documented in your risk analysis records with a named owner, since no fix is coming

Healthcare Sector Incident Watch

H1 2026 Breach Report — Volume Down, Concentration Up

The HIPAA Journal published its H1 2026 Healthcare Data Breach Report on September 30, 2026, based on data obtained from the HHS Office for Civil Rights on September 10. Between January 1



and June 30, 2026, 397 data breaches affecting 500 or more individuals were reported to OCR — a 5.9% decline against H1 2025 and the lowest H1 total since 2023 — with a 22.6% reduction in affected individuals. That is a genuinely positive signal and worth communicating to boards that have been receiving uniformly bad news. It should be read alongside the concentration pattern this series has tracked all year: fewer incidents, but the large ones increasingly occur at vendors and platforms serving many provider organizations at once, as the Oracle Health reporting illustrates. Enforcement also continues — the report notes a joint Massachusetts and Connecticut investigation of Comstar LLC over a breach affecting 585,621 individuals, which identified violations of the HIPAA Security Rule and Massachusetts data security regulations and settled with a \$515,000 financial penalty.

Medical Device and IoT Security

No New Advisory Surfaced — Open Actions Carried

The CISA advisory review for the September 26 to October 2 window surfaced no new ICS Medical Advisory. The most recent remain ICSMA-26-253-01 and ICSMA-26-253-02, both published September 10 and both carrying available vendor fixes, which are now flagged as open actions for a third consecutive cycle and addressed in Priority Action 4. The unpatched standing set is unchanged: Grassroots DICOM reaches week 28 without a fix, pydicom/pynetdicom remains unfixed, and the Pulsetto Vagus Nerve Stimulator has no vendor fix and no vendor response to CISA, meaning undisclosed Bluetooth commands capable of disabling electrical safety mechanisms remain exploitable within radio range with patient counselling as the only available control. Five DICOM product lines carry advisories in total, of which DCMTK, RadiAnt and Orthanc are patchable and should be closed out.

One cross-cutting note from this week's lead item. Citrix NetScaler appliances frequently front clinical remote access, virtual desktop infrastructure and vendor maintenance pathways in healthcare environments. Where a NetScaler appliance provides the remote access route used by medical device vendors for maintenance, a compromised appliance is a medical device security problem as well as an IT one — the same reasoning applied to the BeyondTrust and SimpleHelp items carried in the tracker. Biomedical engineering should be asked which vendor maintenance paths traverse NetScaler infrastructure.

Threat Metrics

Activity Trends	Key Numbers This Week
▲ Edge appliance zero-days under multi-actor exploitation — healthcare GTI-confirmed, exploitation preceding disclosure by weeks ▲ Anti-forensic tradecraft on appliances: log scrubbing, crontab cleaning, spoofed 404 responses ▲ EHR vendor concentration: a single platform breach reaching 29 named health systems ▲ Microsoft Teams as an initial access channel, exploiting the trust gap versus email ▲ Sandbox evasion via hardware telemetry — querying screen refresh rates to detect virtualisation ▼ Large healthcare breach volume DOWN 5.9% year over year in H1 2026, with affected individuals down 22.6% (HIPAA Journal / OCR)	3 days — the CISA KEV remediation deadline for the Citrix zero-days, from September 27 listing to September 30 9.5 CVSSv4 for both CVE-2026-88771 and CVE-2026-88772; 8 vulnerabilities total in Citrix bulletin CTX697096 Sep 9, 2026 — earliest GTIG-tracked exploitation, roughly 18 days before public disclosure 29 health systems named in reporting on the Oracle Health breach 397 large healthcare breaches reported to OCR in H1 2026 — the lowest H1 total since 2023 84 new GTI-verified IOCs; CVE-2026-3650 (GDCM): NO PATCH — week 28

Sources: Google Threat Intelligence (GTI), CISA Alert — Critical Zero-Day Vulnerabilities Exploited in Citrix NetScaler ADC, Gateway (September 27, 2026), CISA KEV Catalog, Citrix Security Bulletin CTX697096, CISA ICS Medical Advisories ICSMA-26-253-01, -253-02, -225-01, -223-01, -223-02, -218-01, -216-01, -181-01, -176-01, -176-02, -083-01, Joint Cybersecurity Advisories AA25-071A, AA26-222A, AA26-231A, AA26-237A, Rapid7, Tenable, watchTower, SecurityWeek, BleepingComputer, NCSC-NL (as reported), Becker's Hospital Review, HIPAA Journal (H1 2026 Healthcare Data Breach Report), HHS Office for Civil Rights, NVD / CVE Program / MITRE, NextGen Healthcare, Orthanc