



Executive Summary

This is an emergency-patching week for a component almost every healthcare organization runs without thinking about it. On October 21, 2026 at 14:00 UTC the PHP project shipped out-of-band security releases 8.5.12, 8.4.27, 8.3.36 and 8.2.35, fixing two critical vulnerabilities — CVE-2026-109618 and CVE-2026-109619, collectively referred to as PHP2SHELL — that allow UNAUTHENTICATED REMOTE CODE EXECUTION. Both are rated CVSS v4.0 9.2. The underlying flaws affect PHP versions 5.4 through 8.5.x in DEFAULT CONFIGURATIONS: hyper-compressed amplification payloads or deserialization paths exhaust the allowed memory limit and trigger an abrupt worker bailout, bypassing normal reference-counting cleanup and creating a Use-After-Free condition when the worker process is reused. PHP's own release notes state plainly that there are no complete mitigations and that updating is the only safe choice. GTIG tracked opportunistic mass scanning ahead of the release and confirmed on October 22 that a public proof-of-concept now achieves full unauthenticated remote code execution against DEFAULT production configurations on Apache mod_php — triggering during initial request handling, without requiring vulnerable application code or an upload endpoint. The exploit does not function against PHP-FPM, which is the single most useful piece of prioritization information available this week.

The healthcare exposure is broad rather than deep. PHP does not usually appear on a clinical application inventory, but it underpins patient portals, practice and hospital websites built on WordPress, legacy clinical and administrative web applications, and the management interfaces of a surprising number of laboratory, imaging and facilities systems. The organizations most at risk are those whose PHP footprint is not centrally owned — marketing-managed websites, departmental applications, and vendor-supplied appliances with embedded web interfaces.

CISA also published a new medical advisory in the window. ICSMA-26-295-01, released October 22, covers CVE-2026-111594 in InterSystems IRIS for Health, a healthcare data platform and interoperability engine: TLS/SSL encryption is turned OFF BY DEFAULT, which may allow an attacker to view transmitted data and use it to log into the device, rated CVSS v3 8.1. This is an insecure default rather than a code defect, so every instance deployed without an explicit hardening step is affected and nothing visibly fails. It is the third healthcare integration or data platform to draw an advisory in six weeks, after NextGen Mirth Connect and J4Care dcm4che. Separately, CISA's published impact detail for the dcm4che advisory is more serious than its initial summary conveyed, and is restated in the tracker below.

Active Threat Campaigns- Healthcare & Technology

Threat Activity	Type	Key Technique / Detail	Targets	Priority Action
PHP2SHELL — Pre-Authenticated RCE in Core PHP (GLOBAL.26.015; CVE-2026-109618 and CVE-2026-109619)	Opportunistic mass scanning and exploitation — multiple actors	Two core PHP memory-safety vulnerabilities affecting PHP 5.4 through 8.5.x IN DEFAULT CONFIGURATIONS. Hyper-compressed amplification payloads or deserialization paths exhaust the allowed memory limit and trigger an abrupt worker bailout, bypassing normal reference-counting cleanup and creating a Use-After-Free condition on worker process reuse — enabling memory disclosure and PRE-AUTHENTICATED REMOTE CODE EXECUTION. PHP shipped emergency releases 8.5.12, 8.4.27, 8.3.36 and 8.2.35 on October 21, 2026 at 14:00 UTC, stating in the release notes that THERE ARE NO COMPLETE	Global event with no industry restriction. Healthcare exposure is broad and indirect: patient portals, WordPress-based practice and hospital sites, legacy clinical web applications, and the administrative web interfaces of many medical and laboratory systems run on PHP	CRITICAL — Patch every PHP runtime to 8.2.35 / 8.3.36 / 8.4.27 / 8.5.12 or later and reload. PHP 8.1 and older are end-of-life and receive NO official fix. Prioritise Apache mod_php deployments; PHP-FPM is not exploitable by the current public exploit but must still be patched



Threat Activity	Type	Key Technique / Detail	Targets	Priority Action
		MITIGATIONS AND UPDATING IS THE ONLY SAFE CHOICE. GTIG tracked opportunistic mass scanning ahead of the release, and on October 22 confirmed a public proof-of-concept achieving FULL UNAUTHENTICATED RCE AGAINST DEFAULT PRODUCTION CONFIGURATIONS on Apache mod_php — triggering during initial request handling without requiring vulnerable application code or upload endpoints, pinning an Apache worker with concurrent connections, and chaining memory disclosure to defeat ASLR. It does NOT function against PHP-FPM		
InterSystems IRIS for Health — TLS Disabled by Default (CISA ICSMA-26-295-01, Oct 22; CVE-2026-111594)	Medical software vulnerability — healthcare data platform	CISA published ICSMA-26-295-01 on October 22, 2026 covering CVE-2026-111594 in InterSystems IRIS for Health. The finding is cleartext transmission of sensitive information: IRIS for Health has TLS/SSL ENCRYPTION TURNED OFF BY DEFAULT, which may enable an attacker to view transmitted data and use that data to log into the device. CVSS v3 is 8.1. InterSystems recommends configuring the IRIS superserver to require TLS. This is a configuration-default problem rather than a code defect, which means every deployment that was stood up without an explicit hardening step is affected, and the exposure persists silently because nothing fails	Healthcare and Public Health. IRIS for Health is a healthcare data platform and interoperability engine used for clinical data storage, HL7 and FHIR messaging, and application hosting — the third healthcare integration or data platform to draw an advisory in six weeks, after Mirth Connect and dcm4che	CRITICAL — Audit every IRIS for Health instance for superserver TLS configuration and enable it. Because the default is insecure, assume unconfigured until proven otherwise, and capture a packet sample to confirm rather than relying on documentation
Citrix NetScaler CVE-2026-88771 — Access Log Poisoning (CAMP.26.162)	Opportunistic exploitation and web shell deployment (motivation unknown)	GTIG has tracked a campaign exploiting Citrix NetScaler Gateway CVE-2026-88771 with activity observed as early as September 8, 2026 — prior to public disclosure. The notable tradecraft is staging: the actor POISONS WEB SERVER ACCESS LOGS by sending HTTP GET requests containing crafted User-Agent headers bearing two-character tags — specifically WK; UL; PX; TR; and 88: — followed by Base64-encoded payloads. The payload is thereby written into the access log, then subsequently extracted from that log, Base64-decoded and executed through a shell. GTIG assesses targeting as opportunistic in nature. This is a distinct cluster from those reported in the October 2 brief and provides materially more specific detection artefacts for the same vulnerability	GTI-confirmed: Aerospace & Defense, Legal & Professional Services — United States. Healthcare NOT confirmed for this cluster, but Healthcare IS GTI-confirmed for GLOBAL.26.012, the multi-actor collection exploiting the same CVE reported October 2	HIGH — Grep NetScaler access logs for the five User-Agent tag prefixes and for Base64 strings in User-Agent fields. This is a retrospective hunt as much as a detection, since exploitation predates disclosure by roughly three weeks



Threat Activity	Type	Key Technique / Detail	Targets	Priority Action
UNC7072 CLOUDHAZE and UNC6767 CURL — Continued Multi-Sector Operations (OP.26.1883, .1884, .1894, .1899)	Targeted intrusion operations — Financial Gain (UNC6767) and Unknown (UNC7072)	Four further single-victim operation records published for two actors this series has tracked since September. UNC7072 continues CLOUDHAZE deployment: OP.26.1883 against a US government organisation (activity August 28 to September 29, intelligence collection) and OP.26.1884 against a US education organisation (activity October 19). UNC6767 continues CURL-based operations: OP.26.1894 against a US education organisation (September 16, data transfer) and OP.26.1899 against a US HEALTHCARE organisation (September 22–23, using the domain spitandmalachite.com). Both actors show sustained, multi-sector operational tempo rather than isolated intrusions	OP.26.1899: Healthcare GTI-confirmed, United States, Financial Gain confirmed. The other three are Government and Education, United States. UNC7072 is the same actor behind the three healthcare victims reported in the October 9 brief	HIGH — Continue blocking and retro-hunting spitandmalachite.com, westbeavers.com, motherotters.com, apexesmasters.com and familypenguins.com. Treat CLOUDHAZE file hashes as a standing EDR retro-hunt across September and October

Top 4 Priority Actions This Week

1. [CRITICAL] Patch Every PHP Runtime — There Is No Mitigation

The PHP project released emergency updates on October 21, 2026 at 14:00 UTC across every supported branch simultaneously: PHP 8.5.12, 8.4.27, 8.3.36 and 8.2.35. The release notes for each are unusually direct, stating that the release fixes two critical vulnerabilities that can allow unauthenticated remote code execution, that all users are strongly encouraged to update immediately, and that THERE ARE NO COMPLETE MITIGATIONS — updating is the only safe choice. CVE-2026-109618 and CVE-2026-109619 are both rated CVSS v4.0 9.2. GTIG's analysis describes the mechanism: hyper-compressed amplification payloads or deserialization paths exhaust the allowed memory limit and trigger an abrupt worker bailout, which bypasses normal reference-counting cleanup and creates a Use-After-Free condition when the worker process is reused, enabling memory disclosure and pre-authenticated remote code execution. GTIG tracked opportunistic mass scanning and attempted exploitation before the patch was available, and on October 22 confirmed that a public proof-of-concept repository had been updated to achieve full unauthenticated RCE against default production configurations on Apache mod_php — triggering during initial request handling without requiring vulnerable application code or upload endpoints, using concurrent connections to pin a single Apache worker, and chaining memory disclosure to bypass ASLR before executing arbitrary commands.

Two pieces of prioritization information matter. First, the working exploit does not function against PHP-FPM, which is how most modern containerized and Nginx-fronted deployments run — so Apache mod_php deployments are the urgent population, though everything still needs patching. Second, PHP 8.1 and older are end-of-life and receive no official fix from the PHP Foundation; PHP 8.2 reaches end of life on December 31, 2026. Healthcare estates carry a disproportionate amount of old PHP because clinical and administrative web applications are long-lived and frequently vendor-supplied.

- Patch every PHP runtime to at least 8.2.35, 8.3.36, 8.4.27 or 8.5.12 for its branch, then reload the service — patching the binary without reloading leaves the vulnerable workers running
- Identify Apache mod_php deployments first; they are exploitable by the current public exploit out of the box. PHP-FPM deployments are not reachable by that exploit but remain vulnerable and must still be patched



- Find the PHP you do not own: marketing-managed websites and patient-facing portals, departmental applications, intranet tools, and vendor appliances with embedded web interfaces. Ask vendors directly whether their product bundles PHP and what their patch timeline is
- For PHP 8.1 and older with no official fix, treat the runtime as end-of-life infrastructure requiring compensating controls or urgent migration — a web application firewall is not a substitute given there are no complete mitigations
- Hunt rather than assume: mass scanning preceded the patch, so review web server logs and process telemetry for unexpected shell spawning from web server workers across the week before and after October 21

2. [CRITICAL] Enable TLS on InterSystems IRIS for Health — It Is Off by Default

CISA published ICSMA-26-295-01 on October 22, 2026, covering CVE-2026-111594 in InterSystems IRIS for Health. The vulnerability class is cleartext transmission of sensitive information, and the finding is stated plainly in the advisory: InterSystems IRIS for Health has TLS/SSL encryption turned off by default, which may enable an attacker to view transmitted data and use that data to log into the device. CVSS v3 is 8.1. InterSystems recommends configuring the IRIS superserver to require TLS. IRIS for Health is a healthcare data platform used for clinical data storage, HL7 and FHIR interoperability, and application hosting — which means the traffic in question is clinical data and authentication material.

Insecure defaults deserve a different response from code defects, and it is worth making the distinction explicit when briefing leadership. There is no patch to deploy and no version number to check. Every instance ever deployed without someone performing an explicit hardening step is affected, the condition is invisible in normal operation because nothing fails, and it will silently reappear on any new deployment, test instance, or disaster-recovery rebuild unless the hardening is baked into the build standard. This is also the third healthcare integration or data platform to draw a CISA advisory in six weeks, after NextGen Mirth Connect on September 10 and J4Care dcm4che on October 15 — a pattern suggesting sustained research attention on the layer that moves clinical data between systems.

- Inventory every InterSystems IRIS for Health instance including development, test, training and disaster-recovery copies, and configure the superserver to require TLS on each
- Verify by packet capture rather than by configuration review — the failure mode here is a setting that was never changed, and documentation frequently describes intent rather than state
- Add 'TLS required on the IRIS superserver' to your build standard and deployment checklist so the default does not silently return
- Review network segmentation around IRIS instances as a compensating control while the configuration work proceeds, and check whether any IRIS traffic traverses links shared with general user networks
- Extend the same question to Mirth Connect and dcm4che deployments: for each healthcare data platform, confirm whether transport encryption is enabled rather than merely available

3. [HIGH] Extend the Citrix Hunt with Access Log Poisoning Artefacts (CAMP.26.162)

GTIG has collected intelligence since September 2026 on a campaign exploiting Citrix NetScaler Gateway CVE-2026-88771, with activity observed as early as September 8 — prior to public disclosure on September 27. The staging technique is the valuable part for defenders. The actor sends HTTP



GET requests containing crafted User-Agent headers bearing two-character tags — WK:, UL:, PX:, TR: and 88: — followed by Base64-encoded payloads. Because the web server writes the User-Agent into its access log, the payload is thereby staged inside the access log itself, from which the actor subsequently extracts it, Base64-decodes it and executes it through a shell. GTIG assesses the targeting as opportunistic, with GTI-confirmed victims in Aerospace & Defense and Legal & Professional Services in the United States; healthcare is not confirmed for this specific cluster, though Healthcare is GTI-confirmed for GLOBAL.26.012, the multi-actor collection exploiting the same vulnerability reported in the October 2 brief.

- Grep NetScaler and fronted web server access logs for the five tag prefixes WK:, UL:, PX:, TR: and 88: appearing in User-Agent fields
- More generally, alert on Base64-looking strings of meaningful length in User-Agent headers — legitimate user agents do not carry encoded payloads, making this a broadly useful detection beyond this campaign
- Extend the retrospective window back to at least early September, before public disclosure, and preserve access logs before any appliance rebuild
- Review whether your log retention on edge appliances actually reaches early September; if not, record that as a limitation on what the hunt can conclude

4. [HIGH] Maintain the UNC7072 and UNC6767 Hunt — Healthcare Targeting Continues

Four further single-victim operation records were published for two actors this series has tracked since September, and both continue to show sustained multi-sector tempo. UNC7072 continues deploying the CLOUDHAZE malware family: OP.26.1883 documents a US government organization with activity from August 28 to September 29 for intelligence collection, and OP.26.1884 a US education organization with activity on October 19. UNC6767 continues CURL-based operations with Financial Gain as a GTI-confirmed motivation: OP.26.1894 documents a US education organization in September using CURL for reconnaissance or data transfer, and OP.26.1899 a US HEALTHCARE organization on September 22–23 using the domain spitandmalachite.com. UNC7072 is the same actor behind the three healthcare victims reported in the October 9 brief, and UNC6767 behind the healthcare victim reported on September 25.

The cumulative picture over six weeks is that two financially or opportunistically motivated actors are working steadily through US healthcare, education and government organizations using ordinary command-line tooling and a small rotating set of domains. Neither relies on novel exploitation. The defensive response is correspondingly unglamorous and durable: maintain the domain blacklist, keep the file hashes in EDR retro-hunt, and alert on the utilities.

- Maintain blocking and periodic retro-hunting for the full UNC7072 and UNC6767 domain set accumulated across this series: spitandmalachite.com, westbeavers.com, motherotters.com, apexesmasters.com and familypenguins.com
- Keep CLOUDHAZE file hashes in a standing EDR retro-hunt covering September and October rather than treating each publication as a one-off ingest
- Alert on curl.exe invoked from unusual parent processes or by accounts with no scripting role on clinical and administrative endpoints — both actors rely on it
- Because UNC6767's motivation is GTI-confirmed as Financial Gain, assume data theft or extortion is the objective and verify that bulk file share and database reads by a single account would be detected



Medical Device and IoT Security

New Advisory — and a More Serious dcm4che Impact Than First Reported

ICSMA-26-295-01 (InterSystems IRIS for Health) is covered in Priority Action 2. One correction and enrichment is warranted on last week's reporting. When the J4Care dcm4che advisory (ICSMA-26-288-02) was covered in the October 16 brief, the available summary described the impact in general terms. CISA's published advisory text is considerably more specific and more serious: successful exploitation could allow an attacker to DELETE STORED MEDICAL IMAGES, disclose patient information, INJECT FORGED STUDIES, REASSIGN PATIENT RECORDS, overwrite files, and cause a denial-of-service condition. Injecting forged studies and reassigning patient records are patient-safety impacts, not data-protection impacts — a forged study in an archive can drive a clinical decision. Combined with a CVSS vector that is network reachable with no privileges and no user interaction, this should be treated as a higher priority than its initial summary suggested. The fix remains release 5.35.2 or later.

The standing position otherwise: NextGen Mirth Connect and Orthanc remain open for a sixth consecutive cycle, with the Mirth Connect downstream credential rotation still the step most likely outstanding. Grassroots DICOM reaches week 31 with no patch, pydicom/pynetdicom remains unfixed, and the Pulsetto Vagus Nerve Stimulator still has no vendor fix and no vendor response to CISA — for these three the recommendation remains formal documented risk acceptance with a named owner rather than indefinite open-finding tracking. Counting dcm4che and Orthanc, seven DICOM-related product lines now carry advisories in the current run.

Threat Metrics

Activity Trends	Key Numbers This Week
▲ Core language runtime under mass exploitation: pre-auth RCE in default PHP configurations with a working public exploit ▲ Insecure-by-default configuration in a healthcare data platform — TLS off unless explicitly enabled ▲ Log poisoning as a payload staging technique on edge appliances ▲ Healthcare integration and data platforms as a sustained advisory theme — third in six weeks ▲ UNC7072 and UNC6767 maintaining multi-sector tempo with repeated healthcare victims ▲ Autonomous AI offensive tooling scaling — ARTEX infrastructure nearly doubled in ten days	9.2 CVSS v4.0 for both PHP flaws; PHP states there are NO complete mitigations — updating is the only safe choice Oct 21, 14:00 UTC — PHP emergency release; Oct 22 — working public exploit against DEFAULT Apache mod_php configurations 5.4 through 8.5.x — the affected PHP version range, in default configurations 5 User-Agent tags to grep in NetScaler access logs: WK; UL; PX; TR; 88: 22 new GTI-verified IOCs; ARTEX grew from 45 to 80 indicators in ten days CVE-2026-3650 (GDCM): NO PATCH — week 31; Mirth Connect and Orthanc open for a sixth week

Sources: Google Threat Intelligence (GTI) and Mandiant, PHP project security releases and GitHub release notes for PHP 8.5.12, 8.4.27, 8.3.36 and 8.2.35 (October 21, 2026), CISA ICS Medical Advisory ICSMA-26-295-01 (October 22, 2026) plus -288-01, -288-02, -253-01, -253-02, -225-01, -223-01, -223-02, -218-01, -216-01, -181-01, -176-01, -176-02, -083-01, CISA ICS Medical Advisory index, CISA ICS Advisories (October 22 Siemens series), CISA KEV Catalog, CISA Alert on BeyondTrust Remote Support (October 16, 2026), BeyondTrust BT26-05, Citrix Security Bulletin CTX697096, Joint Cybersecurity Advisories AA25-071A, AA26-222A, AA26-231A, AA26-237A, InterSystems Corporation, J4Care, watchTower, Laravel, NVD / CVE Program / MITRE