



## Executive Summary

The defining item this week is a federal ransomware advisory that names healthcare first. On August 10, the FBI, CISA, the Department of Defense Cyber Crime Center, the NSA, the US Secret Service, and the Republic of Korea's National Police Agency jointly published AA26-222A on Gunra ransomware. Gunra emerged in April 2025 as a double-extortion variant derived from the leaked Conti source code, and in January 2026 it formalized into a ransomware-as-a-service operation with an affiliate management panel, a configurable builder, cross-platform lockers, and a new branding alias, Golden Community. It is actively recruiting penetration testers as initial access brokers. In the advisory's intended audience section, healthcare and public health is listed ahead of every other sector. Initial access comes through known, patchable vulnerabilities in internet-facing firewall and VPN appliances — the advisory names Fortinet CVE-2024-55591 and CVE-2025-24472, whose exploitation creates a persistent super-user account called forticloud-sync. Two details deserve particular attention from healthcare defenders: the actors have modified virtual desktop authentication files so that one attacker-chosen one-time password always succeeds, creating a durable MFA bypass; and in at least one case they destroyed backup and archived data at both the primary data center and the disaster recovery center before deploying the encryptor.

There is also a genuine recovery opportunity buried in the advisory that is worth surfacing to any organization currently responding to a Gunra incident. As of March 2026, researchers identified a weakness in Gunra's Linux ELF variants — files appended with GNRA — where encryption keys are generated by a weak pseudorandom number generator seeded with the predictable system call srand (time(NULL)). Defenders may be able to mathematically reconstruct the keys from file timestamps and recover data without paying. That makes preservation of encrypted files, file timestamps, ransom notes, and system logs a first-order incident response step rather than an afterthought, and it applies directly to the ESXi and Linux estate that healthcare organizations run underneath clinical workloads.

Elsewhere: CISA published a new medical advisory on August 13 (ICSMA-26-225-01) covering the Flow Neuroscience FL-100 and Halo Neuroscience FL-100 transcranial direct current stimulation headsets, where an undocumented hard-coded credential shared across every device unit allows anyone within Bluetooth range to manipulate brain stimulation parameters and override safety limits — a patient-safety vulnerability rather than a data one. Three new GTI campaigns are reported, none with healthcare confirmed but each with a direct healthcare read-across: Settra ransomware deployed through Palo Alto GlobalProtect CVE-2026-0257 (the same vulnerability this series flagged as CRITICAL on July 3 for healthcare-confirmed espionage), a China-nexus IIS web shell campaign, and an npm dependency-poisoning campaign harvesting cloud and AI service credentials.

### Active Threat Campaigns- Healthcare & Technology

| Campaign / Threat Activity                                                               | Type                                            | Key Technique                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Targets                                                                                                                                                                                                                                                                                 | Priority Action                                                                                                                                                                                                                    |
|------------------------------------------------------------------------------------------|-------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Gunra Ransomware-as-a-Service<br>(Joint CSA AA26-222A, Aug 10; alias "Golden Community") | Financial / Ransomware (RaaS, double extortion) | Conti-derived variant, first observed April 2025, formalised as a RaaS affiliate programme in January 2026 with a management panel, configurable builder, and cross-platform lockers; actively recruits penetration testers as initial access brokers. Initial access via known vulnerabilities in internet-facing firewall and VPN appliances — CVE-2024-55591 and CVE-2025-24472 (FortiOS/FortiProxy authentication bypass), which are used to create a persistent super-user account named forticloud-sync with a hard-coded password — plus SSL-VPN default credentials where account lockout is | Healthcare and public health is the FIRST sector listed in the advisory's intended-audience section, ahead of financial services, critical manufacturing, transportation, government, utilities, academia, media, retail, and professional services. Victims span the Americas, Europe, | CRITICAL — Patch CVE-2024-55591 and CVE-2025-24472 on all FortiOS/FortiProxy estate and hunt for the forticloud-sync account; verify offline immutable backups are held off-domain and off-site; ingest the advisory STIX packages |



| Campaign / Threat Activity                                             | Type                            | Key Technique                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Targets                                                                                                                                                                                                                                                                                                        | Priority Action                                                                                                                                                                                                                                                    |
|------------------------------------------------------------------------|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                        |                                 | absent. Post-access: Impacket psexec/smbclient over SMB, RDP pivots into VDI, secretsdump against domain controllers for NTDS hashes, pass-the-hash and pass-the-ticket, session-cookie hijacking, and modification of VDI authentication files so an attacker-chosen OTP always succeeds — a persistent MFA bypass. Exfiltration of OneDrive and SharePoint via main.exe, archived with 7-Zip/RClone/WinRAR to Mega, up to tens of terabytes. Encryption uses ChaCha20 + RSA-4096, extension .ENCRT, ransom note R3ADM3.txt; volume shadow copies deleted via WMI and backups destroyed at both primary and disaster-recovery sites   | Middle East, Africa, and Asia-Pacific                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                    |
| Settra Ransomware via GlobalProtect CVE-2026-0257 (CAMP.26.111)        | Financial / Ransomware          | Exploitation of CVE-2026-0257 in Palo Alto Networks GlobalProtect VPN, combined with compromised accounts and service credentials, for initial access. The actor pivots internally over SMB and RDP authenticating with elevated privileges, then deploys Settra ransomware. Settra targets network shares, Windows local drives, and ESXi datastores, appending .locked_wip and .locked extensions to victim files. GTI activity window May 12 – July 14, 2026; 13 mapped ATT&CK techniques; intelligence released August 10, 2026                                                                                                    | GTI-confirmed: Manufacturing, Media & Entertainment, Retail — United States. Healthcare NOT confirmed for this campaign. Included because CVE-2026-0257 was the CRITICAL item of the July 3 brief, where Healthcare and Pharmaceuticals were GTI-confirmed for the espionage campaign exploiting the same flaw | CRITICAL — Re-verify GlobalProtect patching against CVE-2026-0257 immediately; the CISA KEV deadline of June 1, 2026 has long passed. Treat any instance unpatched after that date as potentially compromised and hunt before assuming a patch closes the exposure |
| IIS Web Shell Deployment and Potato Privilege Escalation (CAMP.26.112) | Suspected China-nexus intrusion | Compromise of public-facing web servers followed by deployment of multiple PHP and ASPX web shells into targeted directories. CERTUTIL.EXE is used to retrieve follow-on payloads and interactive Bash reverse shells are established for direct command execution. Privilege escalation to SYSTEM is achieved with local exploitation tools from the Potato family — specifically PRINTSPOOFER, SWEETPOTATO, and McpManagementPotato — with discovery commands such as whoami routed to verify elevated access. Activity observed since May 2026, last seen August 8, 2026 — inside this coverage window; 39 mapped ATT&CK techniques | GTI-confirmed: Government, Technology, Transportation — United States, India, Philippines. Healthcare NOT confirmed. Included on technology-relevance grounds: IIS and ASP.NET host patient portals, PACS web front-ends, and vendor integration endpoints throughout healthcare                               | HIGH — Audit internet-facing IIS and web server directories for unauthorized .php and .aspx files; alert on certutil.exe download activity and on Potato-family privilege escalation tooling; this is the second IIS-focused campaign tracked in three weeks       |
| Poisoned NPM Dependencies Deploying Hidden Runtimes (CAMP.26.108)      | Supply Chain / Credential Theft | A widespread npm supply chain attack against a popular dependency ecosystem, followed by deployment of a credential harvester. A malicious post-installation script uses native operating system utilities to silently extract a standalone, architecture-                                                                                                                                                                                                                                                                                                                                                                             | GTI-confirmed: Legal & Professional Services, Retail — United States. Healthcare NOT confirmed. Included on healthcare                                                                                                                                                                                         | HIGH — Audit npm dependency trees and lockfiles in any healthcare-facing application; alert on post-install scripts writing executables to                                                                                                                         |



| Campaign / Threat Activity | Type | Key Technique                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Targets                                                                                                                             | Priority Action                                                                                                                               |
|----------------------------|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
|                            |      | specific JavaScript runtime into a hidden temporary directory; that embedded runtime then executes a heavily obfuscated JavaScript payload nested deep in the project's dependency tree. Once active, the malware spawns shell processes to harvest authentication secrets, cloud credentials, AI service configurations, and cryptocurrency wallets, exfiltrating over encrypted channels to hosting domains and decentralized network infrastructure. GTI activity window July 14 – August 8, 2026 | DevOps relevance: npm dependencies sit inside patient portals, clinical web applications, and integration tooling across the sector | temporary directories and on unexpected JavaScript runtimes; rotate cloud, CI/CD, and AI service credentials from affected build environments |

## Top 3 Priority Actions This Week

### 1. [CRITICAL] Act on the Gunra Ransomware Advisory — AA26-222A

Gunra reaches healthcare through ordinary, patchable edge-device exposure rather than novel tradecraft, which is what makes the advisory actionable. The FBI observed initial access primarily through exploitation of known vulnerabilities in internet-facing devices, naming two FortiOS and FortiProxy authentication bypass flaws, CVE-2024-55591 and CVE-2025-24472. Exploitation abuses scheduled tasks on vulnerable FortiOS firewalls to create a new persistent user account named forticloud-sync carrying super-user privileges and a hard-coded password — an account name every healthcare organisation running Fortinet should search for today. The Korean National Police Agency additionally observed the actors compromising an SSL-VPN appliance through default credentials where account lockout controls were absent, then modifying an unused account to bypass its mandatory password change requirement. From there the actors move by SMB using Impacket psexec and smbclient, pivot over RDP into virtual desktop infrastructure, and dump NTDS from domain controllers with secretsdump for pass-the-hash and pass-the-ticket movement. Two techniques deserve specific defensive attention. First, against one victim the actors modified authentication processing files on the corporate VDI authentication portal so that a specific attacker-designated one-time password value always succeeded, giving them continuous MFA bypass. Second, they deleted backup and archived data at both the primary data centre and the disaster recovery centre, before and after deploying the encryptor. Encryption uses ChaCha20 with RSA-4096, appends .ENCRT, and drops a ransom note in every affected directory; volume shadow copies are deleted through WMI. Exfiltration to OneDrive and SharePoint is performed by a purpose-built executable, main.exe, with archives moved to Mega in volumes reaching tens of terabytes.

- Patch CVE-2024-55591 and CVE-2025-24472 across the FortiOS and FortiProxy estate, then hunt for the forticloud-sync account and any unfamiliar super-user accounts on firewall and VPN appliances regardless of current patch level
- Verify that at least one backup copy is immutable, offline, off-domain, and stored at a site the production Active Directory cannot reach — the destruction of disaster-recovery backups is the single most consequential behaviour in this advisory for clinical continuity
- Audit VDI and remote-access authentication servers for unauthorised modification of authentication processing files, and alert on file integrity changes there; a working MFA prompt is not evidence that MFA is intact
- Review SSL-VPN and network appliance accounts for default credentials, missing account lockout, and accounts whose mandatory password change requirement has been altered
- If you are responding to a Gunra incident involving Linux or ESXi systems (files appended .GNRA), preserve encrypted files, file timestamps, ransom notes, and system logs before any remediation — the advisory documents a weak, time-seeded pseudorandom number generator in the Linux variant that may allow key reconstruction and recovery without payment



- Ingest the AA26-222A STIX XML and JSON packages, and alert on the named tooling where it is not sanctioned in your environment — Impacket, Mimikatz, Sliver, RClone, AnyDesk, MobaXterm, and Amass

## 2. [CRITICAL] Re-verify GlobalProtect CVE-2026-0257 — Now an Espionage AND Ransomware Vector

GTI released CAMP.26.111 on August 10, documenting a financially motivated actor exploiting CVE-2026-0257 in Palo Alto Networks GlobalProtect VPN and deploying Settra ransomware. The actor uses compromised accounts and service credentials for initial access, pivots internally over SMB and RDP authenticating with elevated privileges, and deploys Settra against network shares, Windows local drives, and ESXi datastores, appending .locked\_wip and .locked extensions. GTI confirms Manufacturing, Media & Entertainment, and Retail targeting in the United States; healthcare is not confirmed for this campaign, and this brief does not claim otherwise. The reason it leads the actions list anyway is continuity. CVE-2026-0257 was the CRITICAL item of the July 3 brief, where it was covered as the entry vector for CAMP.26.091, a PRC-nexus espionage campaign for which Healthcare and Pharmaceuticals are both GTI-confirmed targeted industries. That vulnerability carries a CVSS of 9.1, was added to the CISA KEV catalog on May 29, 2026 with a federal remediation deadline of June 1 that has long passed, and has public proof-of-concept exploit code. A single unpatched GlobalProtect portal is now demonstrably reachable by both a state-nexus espionage actor and a ransomware crew. The exposure window has been open for more than two months.

- Re-verify GlobalProtect patch status against CVE-2026-0257 on every portal, including appliances managed by third parties or inherited through acquisition
- Treat any instance that was internet-facing and unpatched after June 1, 2026 as potentially compromised: hunt for unfamiliar local and service accounts, unexpected SMB and RDP authentication from the VPN segment, and new ESXi datastore access patterns
- Protect the hypervisor layer specifically — Settra targets ESXi datastores directly, so verify that ESXi management interfaces are segmented, that lockdown mode is enabled where feasible, and that hypervisor backups are held outside the cluster
- Alert on file extensions .locked\_wip and .locked appearing on network shares, and confirm your file-server monitoring would surface a mass rename before encryption completes

## 3. [HIGH] Close Web Server and Software Supply Chain Exposure

Two GTI records released this week converge on the same lesson from opposite directions. CAMP.26.112 documents a suspected China-nexus actor compromising public-facing web servers since May 2026, with activity last observed August 8. The actor deploys multiple PHP and ASPX web shells into targeted directories, uses CERTUTIL.EXE to retrieve follow-on payloads, establishes interactive Bash reverse shells for direct command execution, and escalates to SYSTEM using Potato-family local privilege escalation tools — PRINTSPOOFER, SWEETPOTATO, and McpManagementPotato — verifying elevated access with whoami. GTI confirms Government, Technology, and Transportation targeting in the United States, India, and the Philippines. This is the second IIS-focused campaign this series has covered in three weeks, after CAMP.26.106 in the July 31 brief, and IIS and ASP.NET sit underneath patient portals, PACS web front-ends, scheduling systems, and vendor integration endpoints across healthcare. CAMP.26.108 comes at the problem from the dependency side: a widespread npm supply chain attack in which a malicious post-installation script uses native operating system utilities to silently extract a standalone JavaScript runtime into a hidden temporary directory, which then executes an obfuscated payload nested deep in the dependency tree. The resulting credential harvester spawns shell processes to collect authentication secrets, cloud credentials, AI service configurations, and cryptocurrency wallets, exfiltrating over encrypted channels. GTI confirms Legal & Professional Services and Retail targeting in the United States. Both sit alongside GLOBAL.26.007, a multi-actor GTI collection covering trojanised NPM and PyPI packages, compromised update mechanisms, and hijacked browser extension developer accounts, with payloads including BEAVERTAIL, TRUFFLEHOG, and QUIETVAULT harvesting



credentials, OAuth tokens, and API keys; GTIG has published dedicated supply chain mitigation guidance alongside it.

- Audit internet-facing IIS and web server content directories for unauthorised .php and .aspx files, comparing against a known-good deployment manifest rather than relying on visual inspection
- Alert on certutil.exe used to download remote content, on Potato-family privilege escalation binaries, and on w3wp.exe or equivalent web server processes spawning command shells — all high-fidelity, low-noise signals
- Audit npm dependency trees and lockfiles for any healthcare-facing application, and alert on post-install scripts that write executables to temporary directories or invoke unexpected JavaScript runtimes
- Rotate cloud, CI/CD, source control, and AI service credentials from any build environment that installed dependencies during the observed activity window, and check whether AI service configuration files are stored where a build process could read them
- Pin dependencies to known-good versions or commit hashes and require review of transitive dependency changes — the payload in CAMP.26.108 was nested deep in the tree, not at the top level

## Medical Device and IoT Security

### New Advisory — Hard-Coded Credentials in Brain Stimulation Headsets (ICSMA-26-225-01)

On August 13, 2026, CISA published ICSMA-26-225-01 covering the Flow Neuroscience FL-100 and Halo Neuroscience FL-100, versions before July 2026. The finding is a use of hard-coded credentials (CWE-798): an undocumented credential, shared by all device units, is authorized to bypass authentication, allowing an attacker within Bluetooth range to arbitrarily manipulate brain stimulation parameters and state, and to override safety limits. CISA lists Healthcare and Public Health as the affected sector, deployment as worldwide, and the manufacturer as Sweden-based. The mitigation is to install the latest firmware through the Flow app. The vulnerability was reported to CISA by A.C. Buglione. Neither a CVE identifier nor a CVSS score surfaced in the sources reviewed for this brief, so none is asserted here.

Two characteristics make this worth escalating beyond a routine tracker entry. First, the credential is shared across every unit, so a single extraction yields access to the entire deployed fleet — there is no per-device compromise ceiling. Second, the consequence is physical rather than informational: the FL-100 is a transcranial direct current stimulation device that delivers low-intensity current to the prefrontal cortex for the treatment of major depressive disorder, and it has been authorized in the United States as an at-home prescription neuromodulation therapy. Manipulating stimulation parameters and overriding safety limits is a patient-harm scenario, and because the device is used at home rather than in a facility, the Bluetooth proximity requirement is a far weaker constraint than it would be inside a controlled clinical environment. Organizations that prescribe, dispense, or supervise these devices should treat firmware currency as a clinical safety task with an owner and a deadline, not an IT backlog item.

- Identify whether your organization prescribes, dispenses, loans, or clinically supervises FL-100 devices, including through behavioral health and community mental health services
- Instruct patients and clinical staff to apply the latest firmware through the Flow app, and confirm completion rather than assuming — at-home devices do not appear in enterprise patch reporting
- Add at-home and patient-owned connected therapeutic devices to your medical device inventory scope; this advisory is a reminder that the estate now extends past the facility perimeter



## Advisory Cadence and the DICOM Backlog

With ICSMA-26-225-01, CISA has now published three medical advisories in ten days after a three-week gap — Thermo Fisher on August 4, Medixant RadiAnt on August 6, and Flow Neuroscience on August 13. The DICOM position is unchanged from last week and remains the standing workload: GDCM (CVE-2026-3650) reaches week 21 with no patch and an unresponsive maintainer, pydicom/pynetdicom (CVE-2026-56445) still has no vendor fix for the same reason, while DCMTK and RadiAnt both have fixes available. Completing the two patchable items and maintaining compensating controls for the two unpatchable ones — blocking DICOM ingestion from unauthenticated sources, imaging network segmentation, boundary file validation, and opening imaging files only from trusted sources — continues to cover all four simultaneously.

## Persistent CVE and KEV Tracker

| CVE / Advisory                                              | System / Component                                                                              | CVSS          | Advisory                                 | Patch   | Status & Action                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------------------------|-------------------------------------------------------------------------------------------------|---------------|------------------------------------------|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ICSMA-26-225-01 (NEW)</b>                                | Flow Neuroscience FL-100 and Halo Neuroscience FL-100 tDCS headsets (versions before July 2026) | Not published | CISA ICSMA-26-225-01 (Aug 13)            | Yes     | Undocumented hard-coded credential, shared across ALL device units, bypasses authentication (CWE-798). An attacker within Bluetooth range can arbitrarily manipulate brain stimulation parameters and state, and override safety limits. Install the latest firmware via the Flow app. Neither a CVE identifier nor a CVSS score surfaced in the sources reviewed for this brief. Reported to CISA by A.C. Buglione. |
| <b>CVE-2024-55591 / CVE-2025-24472 (NEW to this series)</b> | Fortinet FortiOS and FortiProxy (specific versions)                                             | See advisory  | Joint CSA AA26-222A (Aug 10)             | Yes     | Authentication bypass using an alternate path or channel (CWE-288); named in the Gunra advisory as the observed initial access exploits. Exploitation creates a persistent super-user account named forticloud-sync with a hard-coded password. Patch, then hunt for that account across the FortiOS/FortiProxy estate regardless of current patch level.                                                            |
| <b>CVE-2026-0257</b>                                        | Palo Alto Networks GlobalProtect VPN portals                                                    | 9.1           | CISA KEV (deadline Jun 1, 2026 — passed) | Yes     | Now confirmed as the initial access vector for BOTH espionage (CAMP.26.091, July 3 brief) and ransomware (CAMP.26.111, this brief). Re-verify patching; treat instances unpatched after the KEV deadline as potentially compromised.                                                                                                                                                                                 |
| <b>CVE-2026-17583</b>                                       | Thermo Fisher Applied Biosystems genetic analyzers / HID software                               | 8.2 (v4.0)    | CISA ICSMA-26-216-01 (Aug 4)             | Partial | Instrument output files (.fsa/.hid) carry no integrity or authenticity verification, allowing near-undetectable DNA data tampering. Five supported product lines patched with digital signatures; three end-of-life data collection products receive no update — apply file custody and access controls there.                                                                                                       |



| CVE / Advisory                                                           | System / Component                                                       | CVSS                    | Advisory                                    | Patch     | Status & Action                                                                                                                                                                                                                                                  |
|--------------------------------------------------------------------------|--------------------------------------------------------------------------|-------------------------|---------------------------------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE-2026-17264</b>                                                    | Medixant RadiAnt DICOM Viewer ≤ 2025.2                                   | 5.3 (v4.0) / 4.3 (v3.1) | CISA ICSMA-26-218-01 (Aug 6)                | Yes       | Heap out-of-bounds write via crafted JPEG-compressed DICOM pixel data (CWE-787). Update to RadiAnt 2026.1 across all clinical workstations including radiologist home-reading setups.                                                                            |
| <b>CVE-2026-50003 (+4 high)</b>                                          | OFFIS DCMTK Toolkit ≤ 3.7.0 (DICOM library)                              | 9.8                     | CISA ICSMA-26-181-01                        | Yes       | Path traversal via bit-preserving C-GET, plus CVE-2026-50254, -35505, -52868, -44628. Confirm the patched snapshot is deployed and keep pressing imaging vendors on embedded DCMTK timelines.                                                                    |
| <b>CVE-2026-56445</b>                                                    | pydicom / pynetdicom qrscp (DICOM C-STORE)                               | 9.1                     | CISA ICSMA-26-176-01                        | NO        | Unauthenticated path traversal / arbitrary file write. Maintainer remains unresponsive to CISA. Restrict DICOM port access, segment, monitor the GitHub project.                                                                                                 |
| <b>CVE-2026-3650</b>                                                     | Grassroots DICOM (GDCM) 3.2.2                                            | 7.5                     | CISA ICSMA-26-083-01 (Mar 24)               | NO        | Week 21 with no patch. Memory leak parsing malformed DICOM files with non-standard VR types, causing resource depletion and denial of service. Maintain PACS segmentation and block unauthenticated DICOM ingestion.                                             |
| <b>CVE-2026-22879 / CVE-2026-12473</b>                                   | vtk-dicom 9.5.2; OHIF DICOM Web Viewer                                   | 8.1 / 8.2               | Talos TALOS-2026-2366; CISA ICSMA-26-176-02 | Yes       | Heap overflow via crafted DICOM file (vtk-dicom) and SSRF (OHIF, patched v3.12.2). Confirm distribution packages and OHIF deployments are current.                                                                                                               |
| <b>CVE-2025-66376</b>                                                    | Zimbra Collaboration Suite — Classic UI webmail                          | See note                | Joint CSA AA26-204A (Jul 23)                | Yes       | Zero-click XSS exploited by LAUNDRY BEAR since at least July 2025; patched November 2025. Confirm ZCS patch level and hunt with the advisory STIX packages.                                                                                                      |
| <b>CVE-2026-25089 / CVE-2026-39808 / CVE-2026-58644 / CVE-2026-48558</b> | Fortinet FortiSandbox; Microsoft SharePoint Server; SimpleHelp RMM       | 9.8 / 9.1 / 9.8 / KEV   | CISA KEV (Jul 16 / Jun 29)                  | Yes       | Carried KEV items. FortiSandbox exploitation predates its KEV listing — hunt internet-exposed instances. Re-check SharePoint Site Owner assignments on clinical policy libraries and confirm no vendor remote-access path uses an unpatched SimpleHelp instance. |
| <b>CVE-2026-0611 / CVE-2026-43994 / CVE-2024-12248 / CVE-2025-0626</b>   | Spacelabs Sentinel; coturn (telehealth); Contec CMS8000 patient monitors | 9.8 / 8.1 / 9.8         | June briefs; FDA / CISA                     | Yes / N/A | Sentinel v11.6.0 and coturn 4.10.0 patches available — confirm deployment. Contec CMS8000 FDA disconnect recommendation remains in force; no active exploitation observed.                                                                                       |



## Threat Metrics

| Activity Trends                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Key Numbers This Week                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>▲ Federal ransomware advisory naming healthcare first: Gunra RaaS (AA26-222A) — Conti lineage returns to the sector</li><li>▲ Edge device exploitation as the ransomware entry point: Fortinet and Palo Alto flaws both in active ransomware use</li><li>▲ One vulnerability, two actor classes: CVE-2026-0257 now confirmed for espionage AND ransomware</li><li>▲ Medical device patient-safety findings: hard-coded credentials permitting manipulation of brain stimulation parameters</li><li>▲ Software supply chain: two GTI records in one week (npm dependency poisoning and a multi-actor global collection)</li><li>► MFA is no longer a backstop: Gunra actors modified authentication files so an attacker-chosen OTP always succeeds</li></ul> | <p><b>6 agencies co-sealed AA26-222A: FBI, CISA, DC3, NSA, US Secret Service, and the Republic of Korea National Police Agency</b></p> <p>Healthcare and public health listed FIRST among 10 sectors in the Gunra advisory</p> <p>Ransom demands opening at over tens of millions of US dollars; exfiltration volumes up to tens of terabytes</p> <p>33 new GTI-verified IOCs across 4 campaigns, plus the AA26-222A STIX packages</p> <p>3 new CISA medical advisories in 10 days (Aug 4, Aug 6, Aug 13) after a three-week gap</p> <p>CVE-2026-3650 (GDCM): NO PATCH — week 21; CVE-2026-56445 (pynetdicom): NO PATCH</p> |

Sources: Google Threat Intelligence (GTI), Joint Cybersecurity Advisory AA26-222A — #StopRansomware: Gunra Ransomware (FBI, CISA, DC3, NSA, USSS, Republic of Korea National Police Agency, August 10, 2026), CISA ICS Medical Advisories ICSMA-26-225-01, -218-01, -216-01, -181-01, -176-01, -176-02, -083-01, CISA KEV Catalog, Joint Cybersecurity Advisory AA26-204A, US FDA (PMA P230024), Flow Neuroscience, Thermo Fisher Scientific, Medixant, NVD / CVE Program / MITRE, Fortinet PSIRT, Palo Alto Networks, SafeBreach, DataBreaches.net, Water-ISAC