



## Executive Summary

This was an unusually consequential week for healthcare, with three separate SEC-disclosed incidents at organizations the sector depends on. Boston Scientific was hit on August 25 by a cyberattack that took its order-processing and shipping systems offline — the systems used to supply hospitals worldwide with pacemakers, defibrillators, stents and other implantable devices — and disclosed the incident in a Form 8-K filed August 26. Analysts at Piper Sandler, after speaking with management, estimated the disruption could last up to three weeks. This is a clinical availability problem rather than a data breach: no hospital system is touched, but every facility with pending Boston Scientific orders becomes a downstream victim. McKesson, the largest pharmaceutical distributor in the United States, discovered a cybersecurity incident on August 25 involving third-party applications and confirmed unauthorized access and exfiltration of data, after the ShinyHunters extortion group claimed patient data theft. Hospital operator Nutex Health, which runs 28 facilities across 12 states, disclosed via SEC filing that an unauthorized third party accessed and exfiltrated information from its servers. Separately, Toronto's Hospital for Sick Children reported that a flaw in third-party software exposed employee and job applicant data, with clinical systems and patient records unaffected.

On the CISA side, the notable release is one with nothing to patch. Advisory AA26-237A, published August 25 and titled “A Tale of Two SOCs,” documents two simultaneous CISA red team assessments run against consenting critical infrastructure organizations with similar tradecraft. The red team achieved full domain compromise and reached sensitive business systems and cloud resources at BOTH organizations. One never noticed; the other detected and evicted them within minutes. There is no threat actor, no malware family and no indicator list — the tooling was BloodHound, AzureHound, ROADrecon and Rubeus, all publicly downloadable. The privilege escalation chain is worth memorizing because it is endemic in hospital Active Directory: a default Machine Account Quota combined with an ESC1-misconfigured ADCS certificate template takes an unprivileged domain user to a certificate for any identity in the domain. Notably, this series has already seen that technique in the wild — CAMP.26.091 in the July 3 brief used ADCS certificate forging against healthcare-confirmed targets.

Medical device intelligence this week comes from a gap in our own coverage rather than a new release. CISA published no new medical advisory between August 22 and 28, but the review of the ICSMA index for this edition identified two advisories from August 11 that were not covered in the August 14 brief. ICSMA-26-223-02 concerns the Pulsetto Vagus Nerve Stimulator, where undisclosed BLE commands accepted without authentication or encryption allow an attacker to disable electrical safety mechanisms — and Pulsetto has not responded to CISA, so no fix exists. ICSMA-26-223-01 covers the Mira Hormone Monitor and its Android app, with eight CVEs allowing an unauthenticated attacker within BLE range to rebind the device to their own account, extract hormone measurements in cleartext, and passively track the user. Together with the Flow Neuroscience FL-100 advisory covered on August 14, that is three at-home BLE medical devices in three days with authentication failures, two of them permitting override of therapeutic safety limits, and two reported by the same researcher. Details and actions are in the medical device section.

### Active Threat Campaigns- Healthcare & Technology

| Campaign / Threat Activity                                                    | Type                                                      | Key Technique                                                                                                                                                                                                                                                                               | Targets                                                                                                                          | Priority Action                                                                                                                                       |
|-------------------------------------------------------------------------------|-----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| “A Tale of Two SOCs” — CISA Red Team Assessments (Advisory AA26-237A, Aug 25) | Control-effectiveness advisory (no threat actor, no IOCs) | CISA ran two simultaneous red team assessments against consenting critical infrastructure organisations using similar tradecraft, and achieved FULL DOMAIN COMPROMISE plus access to sensitive business systems and cloud resources at BOTH. Against Organization A the team gained initial | Organization A: Government Services and Facilities Sector.<br>Organization B: Water and Wastewater Systems Sector. Healthcare is | CRITICAL — There is nothing to patch and no IOC to block. Set Machine Account Quota to zero, audit ADCS templates for ESC1, and test whether your SOC |



| Campaign / Threat Activity                                                      | Type                                                                                | Key Technique                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Targets                                                                                                                                                                                                                                                                                                                                                             | Priority Action                                                                                                                                                                                                                      |
|---------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                 |                                                                                     | access through a web application using default credentials on several built-in accounts, sent phishing from an internal address, landed on four workstations, escalated over the domain, and moved laterally to sensitive systems and cloud entirely undetected. Organization B detected the activity and shut it down within minutes. The privilege escalation chain that mattered was a default Machine Account Quota combined with an ESC1-misconfigured Active Directory Certificate Services template, which takes an unprivileged domain user to a certificate for any identity in the domain. Tooling was entirely public: BloodHound, AzureHound, ROADrecon and Rubeus | NOT a named sector — carried because the failure modes (default credentials, Machine Account Quota, AD CS misconfiguration, absent detection) are near-universal in hospital Active Directory estates                                                                                                                                                               | would detect this exact sequence                                                                                                                                                                                                     |
| Multi-Actor Exploitation of GlobalProtect CVE-2026-0257 (GLOBAL.26.008)         | Multi-actor tracking collection — Espionage, Financial Gain and Unknown motivations | GTI is tracking MULTIPLE distinct threat actors exploiting CVE-2026-0257 in Palo Alto Networks GlobalProtect VPN to gain initial access. The vulnerability allows unauthorized users to bypass security restrictions and establish a VPN connection. Follow-on activity varies by actor: some deploy additional malware, others perform internal reconnaissance only. The collection carries 20 IP indicators and 66 mapped ATT&CK techniques, and GTI associates it with CVE-2020-1472 (Zerologon) and CVE-2022-26134 (Atlassian Confluence) as onward exploitation, plus five distinct threat actor records. Activity observed from May 12, 2026                             | GTI-confirmed for this collection: Civil Society & Non-Profits, Construction & Engineering, Energy & Utilities, Government, Manufacturing, Media & Entertainment, Retail — United States. Healthcare is not confirmed at collection level, BUT the associated campaign CAMP.26.091 (July 3 brief) has Healthcare and Pharmaceuticals GTI-confirmed for the same CVE | CRITICAL — Third consecutive brief naming this CVE. Verify GlobalProtect patching now; the CISA KEV deadline of June 1, 2026 is nearly three months past. Also verify Zerologon and Confluence patching as onward-exploitation paths |
| CVE-2026-18577 Exploitation Deploying TACTICALRMM and CLOUDFLARED (CAMP.26.121) | Intrusion / Persistence (motivation unknown)                                        | Exploitation of CVE-2026-18577 to deploy TACTICALRMM and CLOUDFLARED binaries for persistence. The actor uses native tools for internal reconnaissance and PowerShell to enumerate Active Directory attributes, and disables Microsoft Defender monitoring through Group Policy and registry modifications to evade detection. Activity observed August 2 – August 6, 2026; 43 mapped ATT&CK techniques; intelligence released August 26, 2026                                                                                                                                                                                                                                 | GTI-confirmed: Legal & Professional Services — United States and Canada. Healthcare NOT confirmed. Carried because the pattern — legitimate RMM deployed for persistence plus Defender disabled via Group Policy — is precisely what the updated federal Medusa advisory documented against healthcare last week                                                    | HIGH — Alert on TacticalRMM and cloudfared binaries where not sanctioned, and on Defender being disabled by Group Policy or registry change. Treat any Defender disablement as an incident, not a configuration drift ticket         |
| Iranian AiTM Phishing Kits Capturing Live MFA Tokens                            | Espionage / Credential Harvesting (Iran-nexus)                                      | A suspected Iranian threat group is running JavaScript-based adversary-in-the-middle phishing kits using spoofed Microsoft Teams meeting invitations, fake OneDrive shared-                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | GTI-confirmed: Civil Society & Non-Profits, Education, Government — Israel, United States,                                                                                                                                                                                                                                                                          | HIGH — Standard MFA does not stop AiTM proxying. Require phishing-resistant FIDO2 or                                                                                                                                                 |



| Campaign / Threat Activity | Type | Key Technique                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Targets                                                                                                                                                                                                                     | Priority Action                                                                                                                                       |
|----------------------------|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| (CAMP.26.123)              |      | document notifications, and account verification alerts. To build victim confidence the actor co-opts legitimate web infrastructure — including compromised WordPress blogs and a Greek government server — to host phishing endpoints and multi-stage redirection chains. The AiTM architecture uses React-based WebSockets to proxy authentication traffic to genuine Microsoft 365 endpoints, harvesting credentials AND capturing dynamic multi-factor authentication tokens in real time. Separate conference-themed infrastructure sharing a unique favicon hash stages typosquatted Microsoft authentication portals. Activity observed to August 9, 2026 | Albania. Healthcare NOT confirmed. Carried because real-time MFA token capture defeats the MFA controls this series recommends, and academic medical centres sit squarely in the research-institution victimology described | certificate-based authentication for clinical and privileged accounts, and add Conditional Access token protection and device compliance requirements |

## Top 4 Priority Actions This Week

### 1. [CRITICAL] Manage Clinical Continuity Through the Boston Scientific Supply Disruption

On August 25, 2026 a cyberattack against Boston Scientific took offline the order-processing and shipping systems the company uses to supply hospitals worldwide with pacemakers, defibrillators, stents and other implantable cardiac and vascular devices. The company disclosed the incident in a Form 8-K filed with the SEC on August 26. Analysts at Piper Sandler, following a conversation with company management, estimated the disruption could last up to three weeks; that is an analyst estimate rather than a company commitment, and should be treated as planning guidance only. The mechanism here is important to communicate accurately to clinical leadership: this is not a breach of hospital systems and not, on current information, a patient data exposure. It is a supply-chain availability event. When a device manufacturer's order-management and shipping infrastructure goes offline, every hospital with pending or in-transit orders becomes a downstream victim without its own systems being touched. Reporting places this as the second major medtech manufacturer in 2026 to have its order-and-shipment layer confirmed as affected, following the Stryker attack covered in this series' March 13 brief, which produced confirmed downstream effects on hospital surgical schedules.

- Task supply chain and cardiac catheterization, electrophysiology and vascular service lines today with an inventory count of Boston Scientific implantable stock on hand, expressed in days of cover at current utilization rather than unit counts
- Identify pending and in-transit Boston Scientific orders and obtain written status; escalate any order supporting a scheduled procedure inside the estimated disruption window
- Activate substitute-device pathways now rather than at the point of shortage: confirm which alternative manufacturers are on contract, whether the substitutes are on formulary, and whether implanting clinicians are credentialed and familiar with them
- Brief perioperative scheduling so that procedure postponement decisions are made deliberately and early, with clinical prioritization, rather than discovered on the morning of a case
- Record this in vendor risk documentation as an availability event, and use it to test whether your business continuity planning covers loss of a single-source device supplier for three weeks — most healthcare continuity plans address loss of IT systems, not loss of a manufacturer's ability to ship

### 2. [CRITICAL] Test Detection Against the AA26-237A Chain — There Is Nothing to Patch



CISA published advisory AA26-237A on August 25, 2026 under the title “A Tale of Two SOC’s: Insights From Two Red Team Assessments.” Under its 6 U.S.C. authority, CISA ran two simultaneous red team assessments in live production environments at two consenting critical infrastructure organizations — Organization A in the Government Services and Facilities Sector and Organization B in the Water and Wastewater Systems Sector — using similar tradecraft. In CISA’s own framing, the red team achieved full domain compromise and accessed sensitive business systems and cloud resources in both environments. Prevention failed comprehensively, twice, at organizations of very different size, funding and regulatory posture. What differed was detection: against Organization A the team gained initial access via a web application using default credentials on several built-in accounts, sent phishing emails from an internal address, landed on four workstations, escalated privileges over the domain, and moved laterally to sensitive systems and cloud resources entirely undetected, while Organization B identified the activity and shut it down within minutes. There is no threat actor to attribute, no malware family, no adversary infrastructure to block, and no IOC list — the red team used BloodHound, AzureHound, ROADrecon and Rubeus, four tools any defender can download this afternoon. The escalation chain that carried the assessment was a default Machine Account Quota combined with an ESC1-misconfigured Active Directory Certificate Services template, which allows an unprivileged domain user to obtain a certificate for any identity in the domain. Healthcare is not a named sector in this advisory, and it does not need to be: default credentials on built-in accounts, an untouched Machine Account Quota and permissive ADCS templates are endemic in hospital Active Directory estates that have grown through acquisition.

- Set the Active Directory Machine Account Quota to zero unless a documented process requires otherwise — the default value of 10 lets any authenticated user create computer accounts, and it is a prerequisite for the escalation path in this advisory
- Audit every ADCS certificate template for the ESC1 misconfiguration: templates that permit requester-supplied subject alternative names combined with client authentication EKU and low enrolment requirements
- Sweep for default credentials on internal web applications, especially built-in and service accounts on appliances, clinical web front-ends and management consoles — this was the initial access route at the organization that never detected the intrusion
- Run the sequence yourself, or have it run, and measure detection at each stage rather than assuming coverage; the honest deliverable from this advisory is a detection-gap report, not a closed ticket
- Treat internally-originated phishing as a distinct detection case — mail sent from a genuine internal address bypasses much of the external-sender logic most organizations rely on

### 3. [HIGH] Address the BLE Medical Device Cluster — Including One With No Fix

Three CISA medical advisories published within three days concern at-home, patient-operated devices whose Bluetooth Low Energy interfaces fail to authenticate, and two of the three permit interference with therapeutic delivery. ICSMA-26-223-02, published August 11, covers the Pulsetto Vagus Nerve Stimulator, all versions, under CVE-2026-18844: the firmware accepts several undisclosed commands over BLE, sent without authentication or encryption and never issued by the companion mobile application, yet fully processed whenever the device is powered on. CISA states that successful exploitation could allow an attacker to use hidden commands to disable electrical safety mechanisms or modify stimulation output settings. Pulsetto has not responded to CISA’s requests to work on mitigation, so there is no fix and no firmware path; CISA directs users to contact the vendor directly. ICSMA-26-223-01, published the same day, covers the Mira Hormone Monitor firmware 1.7.1.47 and Mira Android App 4.5.15.4 from Quanovate Tech, with eight CVEs: a remote unauthenticated attacker within roughly 10 to 30 meters can silently rebind the device to an attacker-controlled account, extract stored hormone measurements in cleartext, cause denial of service through malformed or undocumented command opcodes, and passively track the user because the BLE address never rotates. The third is the Flow Neuroscience and Halo Neuroscience FL-100 advisory covered in the August 14 brief, where a hard-coded credential shared across every unit permits manipulation of brain stimulation parameters and override of safety limits. Two of the



three — Pulsetto and Flow — were reported to CISA by the same researcher, A.C. Buglione, which suggests systematic review of this device class rather than coincidence, and implies more findings are likely.

- Determine whether your organization prescribes, dispenses, recommends, loans or clinically supervises any of these three devices, including through behavioral health, neurology, women's health and fertility services
- For Pulsetto specifically, understand that there is no vendor fix: the only available risk reduction is patient counselling. Advise patients to power the device off when not in active use, since CISA notes the undisclosed commands are processed whenever it is powered on, and to use it in private rather than public settings given the BLE proximity requirement
- For Mira, treat this as a PHI exposure in addition to a device issue — hormone and cycle data is highly sensitive, and the non-rotating BLE address enables physical tracking of the user; check whether your organization recommends this device in any fertility or reproductive health pathway
- Confirm FL-100 firmware updates have actually been applied through the Flow app rather than assuming; at-home devices never appear in enterprise patch reporting
- Formally extend medical device inventory scope to patient-owned and at-home connected therapeutics. Three advisories in three days is a pattern, and this device class sits entirely outside the biomedical engineering asset register at most organizations

#### **4. [HIGH] Close the Remote Access and Authentication Gaps (GLOBAL.26.008, CAMP.26.121, CAMP.26.123)**

Three GTI records this week converge on remote access and authentication. GLOBAL.26.008 elevates CVE-2026-0257 in Palo Alto Networks GlobalProtect from individual campaigns to a multi-actor tracking collection: GTI now tracks multiple distinct threat actors exploiting the same flaw for initial access, with motivations spanning espionage, financial gain and unknown, and associates the collection with CVE-2020-1472 (Zerologon) and CVE-2022-26134 (Atlassian Confluence) as onward exploitation. This is the third consecutive brief naming this CVE — healthcare-confirmed espionage on July 3, Settra ransomware on August 14, and now a multi-actor collection — against a KEV deadline that passed on June 1. CAMP.26.121 documents exploitation of CVE-2026-18577 to deploy TACTICALRMM and CLOUDFLARED for persistence, with Microsoft Defender monitoring disabled through Group Policy and registry modification; GTI does not name the affected product for that CVE, so the exposure cannot yet be scoped, but the behavior is the same pattern the updated federal Medusa advisory documented against healthcare last week. CAMP.26.123 describes a suspected Iranian group running JavaScript adversary-in-the-middle phishing kits that proxy authentication traffic to genuine Microsoft 365 endpoints via React-based WebSockets, harvesting credentials and capturing dynamic MFA tokens in real time, hosted partly on compromised WordPress blogs and a Greek government server, with conference-themed typosquatted portals sharing a common favicon hash.

- Verify GlobalProtect patching against CVE-2026-0257 across every portal including third-party managed and inherited appliances, and confirm Zerologon and Confluence patch status as the documented onward paths
- Inventory and allowlist RMM tooling, then alert on TacticalRMM, cloudflared and any unsanctioned remote access agent — and alert on Microsoft Defender being disabled by Group Policy or registry change, treating it as an incident rather than configuration drift
- Require phishing-resistant authentication (FIDO2 or certificate-based) for privileged, clinical and research accounts — adversary-in-the-middle proxying defeats password-plus-code MFA by design, because the victim authenticates to the real endpoint
- Enable Conditional Access token protection and device compliance requirements so a captured token is not usable from attacker infrastructure, and alert on sign-ins where the token was issued to one device and presented from another



- Brief academic medical centre and research staff specifically: the CAMP.26.123 victimology centres on academic researchers, think tanks and conference-themed lures, and autumn conference season is beginning

## Medical Device and IoT Security

CISA published no new ICS Medical Advisory between August 15 and 21. The most recent remains ICSMA-26-225-01 (Flow Neuroscience and Halo Neuroscience FL-100), released August 13 and covered in full in the previous edition; the firmware update through the Flow app remains outstanding for at-home and clinically supervised devices, and because those devices do not appear in enterprise patch reporting, completion has to be confirmed rather than assumed. CISA did publish two general ICS advisories on August 18 — ICSA-26-230-01 (CISA Malcolm) and ICSA-26-230-02 (Siemens Simcenter Nastran) — neither of which is in medical scope.

The DICOM position is unchanged and remains the standing workload. GDCM (CVE-2026-3650) reaches week 22 with no patch and an unresponsive maintainer; pydicom/pynetdicom (CVE-2026-56445) is in the same position; DCMTK and RadiAnt both have fixes available. Completing the two patchable items and sustaining 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 at once. The Siemens PLC advisory in Priority Action 3 is the medical-device-adjacent item this week: the facilities OT estate sits alongside the clinical estate, and segmentation between them is the control that keeps a building-systems compromise from becoming a clinical one.

## Threat Metrics

| Activity Trends                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Key Numbers This Week                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>▲ Medtech supply-chain disruption: a second major device manufacturer has its order-and-shipment layer taken offline in 2026</li><li>▲ Healthcare vendor and distributor breaches: three SEC-disclosed incidents inside a single week</li><li>▲ BLE medical device authentication failures: a cluster of at-home neuromodulation and monitoring devices, two with safety-limit override</li><li>▲ Detection capability as the deciding control: identical red team tradecraft, opposite outcomes (AA26-237A)</li><li>▲ Real-time MFA token capture via AiTM proxying — standard MFA no longer sufficient for privileged access</li><li>▶ No new CISA medical advisory in this window; the DICOM backlog is unchanged</li></ul> | <p><b>2 organisations, identical tradecraft, FULL domain compromise at both — one detected nothing (AA26-237A)</b></p> <p>Up to 3 weeks estimated disruption to Boston Scientific order and shipping systems (Piper Sandler analyst estimate)</p> <p>28 facilities across 12 states operated by Nutex Health, which disclosed exfiltration via SEC filing</p> <p>9 new medical device CVEs surfaced from two advisories missed in prior windows (1 Pulsetto, 8 Mira)</p> <p>53 new GTI-verified IOCs across 6 campaigns</p> <p>CVE-2026-3650 (GDCM): NO PATCH — week 23; CVE-2026-56445 (pynetdicom): NO PATCH; CVE-2026-18844 (Pulsetto): NO PATCH</p> |

Sources: Google Threat Intelligence (GTI), CISA Cybersecurity Advisory AA26-237A — A Tale of Two SOCs: Insights From Two Red Team Assessments (August 25, 2026), CISA ICS Medical Advisories ICSMA-26-223-01, -223-02, -225-01, -218-01, -216-01, -181-01, -176-01, -176-02, -083-01, CISA ICS Advisory index, CISA KEV Catalog, Joint Cybersecurity Advisories AA25-071A, AA26-222A, AA26-231A, AA26-204A, AA26-097A, US SEC filings (Boston Scientific Form 8-K, McKesson, Nutex Health), Boston Scientific, McKesson, Nutex Health, Hospital for Sick Children (SickKids), Health-ISAC, Piper Sandler (analyst estimate), BleepingComputer, The Hacker News, SafeBreach, TechTimes, PrivacyGuides Data Breach Roundup, NVD / CVE Program / MITRE, Palo Alto Networks, Fortinet PSIRT