## Executive Summary

Three GTI-verified campaigns are reported this week, sourced from Google Threat Intelligence (GTI), CISA, Cisco Talos, and Cisco PSIRT. The most critical is CVE-2026-20182, a maximum-severity (CVSS 10.0, GTI P0) authentication bypass zero-day in Cisco Catalyst SD-WAN Controller and Manager, confirmed exploited in the wild by threat cluster UAT-8616. CISA added it to the Known Exploited Vulnerabilities catalog on May 14 with a federal remediation deadline of May 21, 2026; this is the sixth Cisco SD-WAN vulnerability actively exploited in 2026 alone, representing a sustained, targeted campaign against a technology that sits at the perimeter of many healthcare networks.

Also new this week: CAMP.26.059, a new campaign deploying the VIDAR infostealer via ClickFix lures confirmed targeting Healthcare and Education in the US; and CAMP.26.053, a new persistent intrusion operation using heavily obfuscated PowerShell and in-memory techniques against US healthcare and pharmaceutical organizations, with post-exploitation consistent with pre-ransomware staging. Important context: ClickFix as a technique is not new to this brief series — it was first reported in CAMP.26.017 (February 27 brief) and again in CAMP.26.032 (March 23 brief). CAMP.26.059 and CAMP.26.053 are new campaigns exploiting this well-established vector. CAMP.26.053 is fed by a ClickFix access-broker GTI tracks as UNC6844 (distinct from the April 24 brief's FAKEUPDATES/UNC1543 access-broker, CAMP.25.039, which is a separate cluster). The dominant theme this week: network infrastructure exploitation is converging with healthcare-targeted credential theft, and attackers are combining access brokers with in-memory execution to evade endpoint defenses.

### Active Threat Campaigns- Healthcare & Technology

| Campaign | Type | Key Technique | Targets | Priority Action |
|---|---|---|---|---|
| **Cisco Catalyst SD-WAN Auth Bypass — CVE-2026-20182** *GTI Vulnerability: vulnerability--cve-2026-20182* | Zero-Day / Authentication Bypass | Improper authentication (CWE-287) in SD-WAN peering mechanism; unauthenticated attacker sends crafted DTLS packet to UDP 12346 to gain vmanage-admin access and manipulate NETCONF; SSH key injection; persistent admin access; attributed to UAT-8616; CVSS 10.0 GTI P0 | Healthcare, Technology, Finance, Manufacturing — Global (any org running Cisco Catalyst SD-WAN Controller/Manager) | CRITICAL — Patch immediately (see fixed versions below); CISA KEV federal deadline May 21; if unpatched, assume compromise and hunt for rogue peers and unauthorized SSH keys |
| **VIDAR Infostealer via ClickFix / NEONSLIDE Downloader** *GTI Campaign: CAMP.26.059 — NEW campaign; ClickFix technique previously reported Feb 27 (CAMP.26.017) and Mar 23 (CAMP.26.032)* | Credential Theft / Initial Access | Watering hole + fake Cloudflare verification lure (ClickFix — continued escalating vector); victims deceived into running malicious PowerShell in terminal; NEONSLIDE downloader fetches secondary payload from rotating C2 infrastructure; randomized staging directories + immediate file deletion to minimize on-disk footprint; deploys VIDAR infostealer. Note: ClickFix technique first reported CAMP.26.017 (Feb 27 brief); this is a new campaign using the same social engineering method. | Healthcare, Education — US (GTI confirmed; active since March 23, last seen May 13, 2026) | HIGH — Block PowerShell execution from browser-prompted commands; train staff on ClickFix lures; deploy DNS filtering against NEONSLIDE C2 domains |
| **Obfuscated PowerShell Pre-Ransomware Staging** *GTI Campaign: CAMP.26.053 — NEW campaign; fed by ClickFix initial access (see* | Espionage / Ransomware Precursor | ClickFix initial access (same technique as CAMP.26.017/CAMP.26.032 in prior briefs, attributed here to UNC6844); heavily obfuscated Base64-encoded PowerShell downloads in-memory payloads; ASEP Run key persistence; malicious DLLs + CSC.EXE on-disk compilation; post-exploitation: SYSTEMINFO, IPCONFIG, NLTEST | Healthcare, Pharmaceuticals, Government, Education, Manufacturing — US (GTI confirmed; first seen April 13, 2026) | HIGH — Alert on Base64-encoded PowerShell with HttpClient; audit RunMRU and ASEP registry keys; treat any SYSTEMINFO/NLTEST pattern post-PowerShell as active pre-ransomware indicator |

| Campaign | Type | Key Technique | Targets | Priority Action |
|---|---|---|---|---|
| *CAMP.26.059 above)* | | discovery consistent with pre-ransomware staging. Note: CAMP.26.055 referenced in GTI as the UNC6844 access-broker campaign — distinct from the Apr 24 brief's CAMP.25.039 (FAKEUPDATES/UNC1543) despite similar access-broker function. | | |

# Top 3 Actions This Week

## 1. [CRITICAL] Patch Cisco Catalyst SD-WAN CVE-2026-20182 — Maximum-Severity Zero-Day Authentication Bypass

On May 14, 2026, Cisco published advisory cisco-sa-sdwan-rpa2-v69WY2SW confirming active exploitation of CVE-2026-20182, a critical improper authentication vulnerability (CWE-287) in the peering authentication mechanism of Cisco Catalyst SD-WAN Controller (formerly vSmart) and Cisco Catalyst SD-WAN Manager (formerly vManage). The vulnerability carries a CVSS score of 10.0 and is rated GTI Priority P0. An unauthenticated remote attacker can exploit the flaw by sending a specially crafted DTLS challenge acknowledgment packet containing a forged vHub device-type certificate and an empty signature block to UDP port 12346, triggering an improper conditional jump in the vbond_proc_challenge_ack function that bypasses peer verification entirely.

Healthcare organizations: Cisco Catalyst SD-WAN devices are commonly deployed as healthcare network perimeter devices and WAN edge for multi-site clinical environments. A root-level compromise of these devices allows an attacker to intercept all WAN traffic, including HL7/FHIR clinical data flows, and pivot into clinical VLANs and medical device networks.

### Fixed Versions (apply immediately):

- 20.9.x → 20.9.9.1 | 20.12.x → 20.12.5.4 / 20.12.6.2 / 20.12.7.1
- 20.15.x → 20.15.4.4 / 20.15.5.2 | 20.18.x → 20.18.2.2 | 26.1.x → 26.1.1.1
- Cloud-managed (SD-WAN Cloud, Cisco Managed): update 20.15.506 applied automatically — no action required

### Immediate Actions:

- Inventory all Cisco Catalyst SD-WAN Controllers and Managers; verify version against the fixed list above
- If unpatched: treat the device as potentially compromised — do not wait; engage incident response and look for unauthorized SSH keys and rogue SD-WAN peers
- Run 'request admin-tech' on each control component before upgrading to preserve indicators of compromise
- Review NETCONF audit logs for unexpected configuration changes, new vHub peer registrations, or admin account modifications
- Apply Cisco IPS signatures and review Talos SD-WAN Threat Hunt Guide for detection artifacts
- Restrict management-plane access to SD-WAN controllers — these should never be internet-reachable; place behind jump hosts or VPN

## 2. [HIGH] Block VIDAR Infostealer Campaign — New ClickFix Campaign Targeting Healthcare (CAMP.26.059)

*NOTE: ClickFix as a social engineering technique has been reported in this brief series before multiple times. CAMP.26.059 is a new, distinct campaign using the same lure method, with new infrastructure, a new downloader (NEONSLIDE), and a new final payload (VIDAR). If ClickFix controls were deployed following prior briefs, verify they remain in place and effective against this variant.*

Active since March 23, 2026, and last confirmed active May 13, 2026, GTI campaign CAMP.26.059 is a watering-hole and ClickFix social engineering campaign confirmed targeting Healthcare and Education

organizations in the United States. The attack chain begins with compromised legitimate websites that display fake Cloudflare CAPTCHA verification pages. The ClickFix technique deceives users into manually copying a malicious PowerShell command from the fake verification page and pasting it directly into their terminal. The NEONSLIDE PowerShell downloader then executes with hidden window parameters, contacts a rapidly rotating command-and-control infrastructure, downloads the final payload to a randomized staging directory, and immediately deletes the executable artifacts to minimize on-disk forensic evidence.

The final payload is VIDAR, a well-established infostealer that harvests browser credentials, saved passwords, session cookies, and other sensitive data. VIDAR is particularly dangerous in healthcare environments because clinical staff commonly use browsers to access EHR portals, insurance portals, and clinical decision support systems, meaning stolen credentials can enable direct access to PHI and administrative healthcare systems.

### Actions:

- Block outbound PowerShell execution from browser processes (Edge, Chrome, Firefox) via AppLocker or equivalent endpoint policy
- Train all clinical and administrative staff on ClickFix social engineering: legitimate verification pages never ask users to run terminal commands
- Deploy DNS filtering to block known NEONSLIDE C2 domains — obtain full IOC list from GTI portal under CAMP.26.059 (9 domains, 2 IPs, 13 URLs)
- Alert on: Base64-encoded PowerShell executions with hidden window flags (-WindowStyle Hidden), PowerShell spawned from browser processes, randomized temp-directory executable creation followed by immediate deletion
- If VIDAR is detected, treat as a full credential compromise event: rotate all affected user credentials and invalidate active sessions

## 3. [HIGH] Detect and Contain Pre-Ransomware PowerShell Staging in Healthcare (CAMP.26.053)

*CAMP ID CLARIFICATION: GTI references a campaign designated CAMP.26.055 (UNC6844) as the ClickFix access-broker that seeds CAMP.26.053. This should not be confused with the April 24 brief entry also labeled CAMP.26.055, which referred to the UNC1543 FAKEUPDATES/FakeUpdates drive-by campaign (GTI canonical ID CAMP.25.039). Both are access-broker operations using social engineering but involve different actors, different lure infrastructure, and different downstream payloads. They are not the same campaign.*

GTI CAMP.26.053, active since April 13, 2026, represents a sophisticated targeted intrusion operation against US healthcare, pharmaceutical, government, and education organizations. Initial access is delivered via a ClickFix campaign attributed to UNC6844, which hands off the foothold to a secondary actor deploying the main payload. Post-access, the attacker uses heavily obfuscated, Base64-encoded PowerShell to download payloads directly into memory, evading file-based antivirus entirely. Persistence is established via Windows Registry ASEP Run keys, with malicious DLLs also dropped and the native C# compiler (CSC.EXE) used to compile code on disk.

Post-exploitation activity includes extensive system and network discovery using SYSTEMINFO, IPCONFIG, and NLTEST — a pattern GTI identifies as consistent with pre-ransomware reconnaissance. This campaign directly links to the broader ClickFix + ransomware precursor pipeline. Healthcare and pharma organizations should treat any detection of this activity pattern as an active ransomware precursor requiring immediate containment.

### Actions:

- Re-prioritize SIEM rules: PowerShell spawning with Base64-encoded payloads that include HttpClient strings should be Priority-1; do not treat as background noise
- Alert on ASEP Run key creation by non-standard processes; audit all current Run key entries for unexpected entries
- Alert on CSC.EXE execution outside of known developer environments; this is a red flag for on-disk payload compilation in clinical environments

- Hunt for SYSTEMINFO + IPCONFIG + NLTEST executed in sequence from the same process tree within minutes of a PowerShell download event — this pattern is a high-fidelity pre-ransomware indicator
- Ensure EDR behavioral coverage is active on all clinical workstations, EHR terminals, pharmacy systems, and nursing-station endpoints

## Medical Device and IoT Security

### Cisco SD-WAN — Direct Relevance to Clinical Networks

CVE-2026-20182 carries direct medical device implications. Cisco Catalyst SD-WAN is used in multi-site healthcare organizations to connect hospitals, clinics, and data centers. A compromised SD-WAN controller gives an attacker the ability to intercept all inter-site clinical traffic, including unencrypted HL7 messages, DICOM imaging transfers, and remote access sessions used by medical device vendors for maintenance and patching.

- Audit which medical device vendors use SD-WAN-connected remote access paths for maintenance; a compromised controller could expose these sessions
- Verify clinical VLAN segmentation is enforced at the WAN edge independently of SD-WAN policy to ensure a compromised controller cannot collapse network isolation

### Persistent Medical Device Advisories (No Change This Week)

CVE-2026-3650 (GDCM DICOM Memory Leak): No patch available as of May 15, 2026. CISA advisory ICSMA-26-083-01 remains open. Continue network segmentation of PACS and imaging systems. Block unauthenticated DICOM connections.

Contec CMS8000 / Epsimed MN-120 (CVE-2024-12248, CVE-2025-0626): FDA disconnect recommendation unchanged. GTI EPSS 0.0068, no active exploitation confirmed.

BeyondTrust CVE-2026-1731: Confirm patching is complete across all vendor remote-access platforms used for medical device maintenance. Treat any unpatched BeyondTrust appliance as compromised.

Ivanti EPMM CVE-2026-38125 (from May 1 brief): CISA KEV deadline was April 29. Verify all instances are patched to 12.4.0.1+.

*Sources:Google Threat Intelligence (GTI) Cisco Systems Inc. / Cisco Talos | CISA | MITRE ATT&CK | National Vulnerability Database | BleepingComputer | The Hacker News | SecurityWeek | Dark Reading | Tenable Blog | eSecurityPlanet*