



Executive Summary

The dominant item is an actively exploited zero-day in a remote-support appliance that healthcare organizations routinely expose to vendors. On October 15, 2026 BeyondTrust disclosed CVE-2026-102764, a critical authentication bypass by spoofing in Remote Support, formerly Bomgar, affecting all versions through 26.2.3 and carrying a CVSSv4 score of 9.3. Internal Remote Support components inadequately validate the origin of incoming messages, allowing an unauthenticated remote attacker to perform arbitrary file operations on the appliance with no user interaction. CISA added it to the Known Exploited Vulnerabilities catalog on October 16 with a federal due date of October 19 and forensic triage marked as required, stating that actors are actively exploiting it to gain initial access and then establish persistence, escalate privileges and move laterally. The critical detail comes from the incident response: Mandiant, part of Google Threat Intelligence Group, found that a threat actor exploited this flaw AS A ZERO-DAY beginning August 29, 2026 — nearly seven weeks before disclosure. BeyondTrust names the actor ARMORY CASTLE and reporting attributes it to a suspected China-nexus espionage cluster. This is now the SECOND critical BeyondTrust remote-access flaw in this tracker, after CVE-2026-1731 which was the CRITICAL item of the April 17 brief and was later named in the federal Medusa advisory.

Medical device advisory cadence resumed with two new ICSMAs published on October 15. ICSMA-26-288-02 covers four vulnerabilities in J4Care dcm4che (dcm4chee-arc-light 5.35.1), a widely deployed open-source DICOM archive, rated CVSS v3.1 9.1 CRITICAL with a vector that is network reachable, requires no privileges and no user interaction, and carries high integrity and availability impact; the flaws comprise missing authorization, an infinite loop condition, inefficient algorithmic complexity and missing authentication for a critical function, fixed in release 5.35.2. ICSMA-26-288-01 covers CVE-2026-107777 in Thermo Fisher Torrent Suite Software versions 5.18 and earlier, a path traversal allowing an attacker to read arbitrary files on the Torrent Server, fixed in 5.22. dcm4che is the sixth distinct DICOM product line to draw a CISA advisory in the current run, and Torrent Suite is the second Thermo Fisher genomics product after the Applied Biosystems integrity flaw in August.

On the campaign side, CAMP.26.160 is GTI-confirmed for Healthcare among five industries and documents a notable living-off-the-land technique: phishing lures masquerading as Zillow rental and tenant verification requests lead to ClickFix landing pages that have victims paste commands into the Windows command prompt, with heavy caret-based obfuscation and abuse of the native FINGER.EXE utility to download payloads. CAMP.26.161 targets the managed service provider trust relationship directly, abusing compromised service principal credentials for ConnectWise Cloud Backup (SkyKick) to reach downstream Microsoft 365 tenants and self-assign Global Administrator roles. And GLOBAL.26.014 documents multiple actors abusing ARTEX, an autonomous AI-driven penetration testing framework — the second autonomous AI offensive capability this series has reported in four weeks.

Active Threat Campaigns- Healthcare & Technology

Threat Activity	Type	Key Technique / Detail	Targets	Priority Action
BeyondTrust Remote Support Zero-Day — CVE-2026-102764 <i>(CISA alert and KEV, Oct 16; actor ARMORY CASTLE)</i>	Nation-state espionage (suspected China-nexus) — exploited as a zero-day	A critical authentication bypass by spoofing (CWE-290) in BeyondTrust Remote Support, formerly Bomgar, affecting ALL versions through 26.2.3. Internal Remote Support components inadequately validate the origin of incoming messages, permitting an unauthenticated remote attacker to	Any organisation running self-hosted BeyondTrust Remote Support or Privileged Remote Access. Direct healthcare exposure: this series has repeatedly flagged	CRITICAL — Apply BT26-05-RS now; self-hosted versions older than 24.3.1 must upgrade first. Then follow CISA's explicit instruction: ROTATE EVERY CREDENTIAL the appliance stored



Threat Activity	Type	Key Technique / Detail	Targets	Priority Action
		perform arbitrary file operations on the appliance with no user interaction.	BeyondTrust as a medical device vendor remote-access path, and CVE-2026-1731 in the same product was the CRITICAL item of the April 17 brief	or injected, revoke all active support sessions, and review new MFA registrations on privileged accounts
Zillow-Themed ClickFix Lures Abusing finger.exe (CAMP.26.160)	Social engineering initial access (motivation not assigned)	Between mid and late September 2026 an unknown actor ran widespread social engineering and initial access campaigns against multiple organizations across the United States and the United Kingdom. Initial access came through phishing email lures masquerading as legitimate ZILLOW RENTAL AND TENANT VERIFICATION REQUESTS, directing victims to fraudulent ClickFix-style landing pages that instructed them to copy and paste malicious commands directly into the Windows command prompt under the pretext of resolving a technical verification issue.	Healthcare GTI-confirmed, among five industries (also Education, Energy & Utilities, Manufacturing, Oil & Gas) — United States confirmed, with the campaign description also citing the United Kingdom	HIGH — Block or alert on finger.exe execution, which has essentially no legitimate modern use and is a highly reliable detection. Alert on caret-heavy command strings and on clipboard-pasted commands in cmd.exe; refresh ClickFix training with the rental-verification pretext
ConnectWise Cloud Backup Service Principal Abuse → Microsoft 365 Tenants (CAMP.26.161)	Managed service provider supply chain compromise (motivation undetermined)	Since October 2026 GTIG has tracked a campaign abusing COMPROMISED SERVICE PRINCIPAL CREDENTIALS for the ConnectWise Cloud Backup (SkyKick) application to gain initial access to DOWNSTREAM MICROSOFT 365 TENANTS. Public reporting indicates that following a successful OAuth 2.0 client credentials flow to acquire Microsoft Graph API tokens, the actor escalates privileges by manipulating ConnectWise applications to SELF-ASSIGN Global Administrator and Exchange Administrator roles.	GTI-confirmed: Legal & Professional Services — United States. Healthcare NOT confirmed. Carried because the attack path is the managed service provider trust relationship itself, which is how a large share of healthcare organizations consume backup, M365 administration and security services	CRITICAL (if you or your providers use ConnectWise Cloud Backup / SkyKick) — Audit enterprise application service principals in every M365 tenant for unexpected client secrets, recent Global or Exchange Administrator role assignments, and Graph API activity from unfamiliar user-agents
ARTEX Autonomous AI Penetration Testing Framework Abused by Multiple Actors (GLOBAL.26.014; also tracked as ScopeWeaver)	Multi-actor tooling abuse — Unknown and Financial Gain (China source region)	GTIG collected intelligence on multiple threat actors abusing ARTEX, an AUTONOMOUS AI-DRIVEN PENETRATION TESTING FRAMEWORK built on the Norma v0.4 agent engine. ARTEX orchestrates automated reconnaissance using ScopeSentry, local TLS man-in-the-middle proxy inspection, headless Chrome browsing, and iterative exploit execution tagged with sequential intent-IDs — in other words, the framework reasons about and retries its own exploitation attempts. Observed operations include Weaver Ecology OA SQL injection and MySQL general_log_file poisoning to deploy JSP micro-webshells, abuse of Azure	GTI-confirmed: Chemicals & Materials, Construction & Engineering, Government, Manufacturing, Technology — United States. Healthcare NOT confirmed. Carried as a technology development: this is the second autonomous-AI offensive capability this series has reported, after the	HIGH (strategic) — Assume web application attack surface will now be probed continuously and systematically rather than opportunistically. Prioritize authenticated API authorization testing (IDOR and mass assignment) and alert on webhook.site egress



Threat Activity	Type	Key Technique / Detail	Targets	Priority Action
		App Service Kudu VFS and command APIs, automated API IDOR, local file inclusion and mass-assignment probing, and staging and exfiltration via webhook.site. The record carries 117 mapped ATT&CK techniques and 45 indicators including 36 IP addresses; activity observed July 16 to October 9, 2026	Services Australia agent incident in the September 25 brief	

Top 4 Priority Actions This Week

1. [CRITICAL] Patch BeyondTrust Remote Support and Assume Compromise Back to August

CVE-2026-102764 is the most consequential item this series has reported on a remote-access appliance, and the timeline is why. BeyondTrust shipped the BT26-05 patch to hosted and self-hosted customers on October 8 and automatically applied it to all Remote Support and Privileged Remote Access SaaS tenants by October 9. Coordinated public disclosure followed on October 15. CISA issued its alert and added the flaw to the KEV catalog on October 16, setting a federal remediation due date of October 19 — three days — and marking forensic triage as required. But the exploitation predates all of that: during an incident response engagement Mandiant found evidence that a threat actor had exploited the vulnerability as a zero-day, with first exploitation dated August 29, 2026. That is nearly seven weeks of exploitation before any patch existed. BeyondTrust names the actor ARMORY CASTLE; reporting attributes the activity to a suspected China-nexus espionage cluster, and CISA states actors are using the flaw to gain initial access and then establish persistence, escalate privileges and move laterally. Two compromises are publicly known so far, one BeyondTrust-hosted instance and one self-hosted appliance, but the exposure window means absence of a known compromise is not reassurance.

- Apply the BT26-05-RS patch immediately to all self-hosted Remote Support appliances; organizations running a version older than 24.3.1 must upgrade to a newer version before the patch can be applied, which makes this a change-window problem as well as a patching one
- Apply the patch to Privileged Remote Access as well — BeyondTrust states its testing found no exploitation path in PRA, but PRA shares the affected code and the vendor released the patch out of caution
- Follow CISA's explicit post-patch instruction, which is unusually prescriptive: ROTATE EVERY CREDENTIAL the appliance stored or injected, REVOKE all active support sessions, and REVIEW new multifactor authentication registrations on privileged accounts
- Conduct forensic triage rather than assuming a clean appliance — CISA marks this as required in the KEV entry. Hunt for the Remote Support service spawning unexpected shells, unauthorized file uploads to the appliance, and new administrative accounts, covering the period from late August forward
- Restrict external access to the appliance and limit administrative interfaces to trusted networks, as CISA directs; a remote-support appliance reachable from the internet is the exposure that makes this exploitable



- Ask every medical device and IT vendor that uses BeyondTrust to reach your environment to confirm in writing that their appliance is patched and triaged — your own remediation does not cover a vendor-operated appliance that terminates inside your network

2. [CRITICAL] Remediate the Two New Medical Advisories — Including a Critical DICOM Archive Flaw

CISA published two medical advisories on October 15. ICSMA-26-288-02 is the more serious: four vulnerabilities in J4Care dcm4che, specifically dcm4chee-arc-light version 5.35.1, rated CVSS v3.1 9.1 CRITICAL and v4.0 8.8 HIGH. The weaknesses are Missing Authorization (CWE-862), Loop with Unreachable Exit Condition (infinite loop), Inefficient Algorithmic Complexity, and Missing Authentication for Critical Function. The CVSS vector deserves attention when briefing clinical leadership: AV:N/AC:L/PR:N/UI:N with high integrity and availability impact means network reachable, low attack complexity, no privileges required and no user interaction, with the consequence being modification of data and denial of service rather than disclosure. dcm4che is a widely deployed open-source DICOM archive and PACS platform, frequently used in research imaging, teaching hospitals and as a routing and archive tier in production estates. J4Care has provided a fix in release 5.35.2 or later. With this advisory, six distinct DICOM product lines now carry CISA advisories in the current run — GDCM, pydicom/pynetdicom, DCMTK, RadiAnt, Orthanc and now dcm4che — spanning libraries, viewers, servers and archives.

- Inventory dcm4che and dcm4chee-arc-light deployments across clinical, research and teaching environments, including instances stood up by imaging or research teams outside IT procurement, and update to release 5.35.2 or later
- Because the dcm4che flaws require no authentication and no user interaction, prioritise any instance reachable from a general clinical VLAN or the internet; network reachability is the whole exposure here
- Inventory Thermo Fisher Torrent Suite Software across genomics and molecular diagnostics laboratories and update to 5.22 or later; note that exploitation requires low privileges, so review who holds accounts on the Torrent Server
- Treat the six-product DICOM position as a single program rather than six tickets: the shared control set — blocking DICOM ingestion from unauthenticated sources, imaging network segmentation, boundary file validation, and opening imaging files only from trusted sources — covers all of them, and four of the six now have fixes available
- Brief biomedical engineering and laboratory leadership that the advisory pattern has now extended from imaging into genomics instrumentation across two separate Thermo Fisher products

3. [HIGH] Block finger.exe and Refresh ClickFix Training (CAMP.26.160)

GTIG documented a widespread social engineering and initial access campaign running from mid to late September 2026 against organizations across the United States and the United Kingdom, spanning higher education, healthcare and commercial sectors, with Healthcare GTI-confirmed among five targeted industries. The lure is specific and unusual: phishing emails masquerading as legitimate Zillow rental and tenant verification requests, directing victims to fraudulent ClickFix-style landing pages that instruct them to copy and paste commands into the Windows command prompt under the pretext of resolving a technical verification issue. The executed commands use heavy caret-based string obfuscation — inserting caret characters to break up command strings and defeat naive signature matching — and abuse the native Windows FINGER.EXE utility to



download initial payloads from adversary-hosted infrastructure, then stage execution structures and loops to unpack and launch secondary and final payloads. GTIG notes candidly that none of those later-stage payloads have been observed in any successful network compromise to date, so the end objective is not established.

- Block finger.exe by application control policy where possible, and alert on its execution everywhere else — this is close to a zero-false-positive detection in a managed clinical environment
- Alert on command lines containing unusual density of caret characters, and on cmd.exe processes whose command line arrives via clipboard paste
- Refresh ClickFix awareness training with this specific pretext — a rental or tenant verification request is a personal-life lure that reaches staff through their own concerns rather than their work role, which is why it works
- Reinforce the standing message that no legitimate website or verification process ever asks a user to paste a command into the Run dialog or a command prompt
- Ingest the two domains and four URLs from the GTI record into web filtering

4. [HIGH] Audit Service Principals and Managed Provider Trust (CAMP.26.161)

GTIG has tracked a developing campaign since October 2026 abusing compromised service principal credentials for the ConnectWise Cloud Backup (SkyKick) application to gain initial access to downstream Microsoft 365 tenants. Following a successful OAuth 2.0 client credentials flow to acquire Microsoft Graph API tokens, the actor escalates privileges by manipulating ConnectWise applications to self-assign Global Administrator and Exchange Administrator roles. Observed tradecraft includes a variety of user-agents for automated tenant enumeration, curl for password spraying, and kiota-dotnet — a Microsoft Graph SDK component — for role assignments. For persistence the actor adds new client secrets to enterprise applications, establishing redundant long-term access, then reads and writes data across Exchange, SharePoint, OneDrive and Teams. GTI confirms Legal & Professional Services targeting in the United States; healthcare is not confirmed and this brief does not claim it is. It is carried because the attack path is the managed service provider trust relationship itself, which is how a substantial share of healthcare organizations consume backup, Microsoft 365 administration and security services.

- Enumerate every enterprise application and service principal in your Microsoft 365 tenants, identify which hold Global Administrator, Exchange Administrator or broad Graph permissions, and confirm each is still required
- Alert on new client secret or certificate addition to any enterprise application, and on role assignments made by a service principal rather than a user — both are the documented persistence and escalation steps
- Alert on Graph API activity from unfamiliar user-agents and on kiota-dotnet role assignment calls outside known automation
- Ask your managed service and backup providers directly whether they use ConnectWise Cloud Backup or SkyKick in delivering your service, and what their service principal credential rotation and monitoring practice is
- Review conditional access and workload identity policies: service principals are frequently exempt from the controls applied to user sign-ins, which is precisely why this path works



Medical Device and IoT Security

Two New Advisories — DICOM Archive and Genomics Instrumentation

Both new advisories are covered in full in Priority Action 2. The tracker position after this week: ICSMA-26-288-02 (J4Care dcm4che, CVSS v3.1 9.1 critical, fix in release 5.35.2) and ICSMA-26-288-01 (Thermo Fisher Torrent Suite Software, CVE-2026-107777, fix in 5.22) are both patchable and newly open. The two September 10 advisories — NextGen Healthcare Mirth Connect and Orthanc DICOM Server — are now open for a fifth consecutive reporting cycle, with the Mirth Connect downstream credential rotation still the step most likely to be outstanding. The permanently unfixable set is unchanged: Grassroots DICOM reaches week 30 with no patch, pydicom/pynetdicom remains unfixed, and the Pulsetto Vagus Nerve Stimulator has no vendor fix and no vendor response to CISA.

Two observations for planning. First, the DICOM advisory run has now reached six distinct product lines and has moved through every tier of the imaging stack — parsing libraries (GDCM, pydicom/pynetdicom, DCMTK), clinical viewers (RadiAnt, OHIF), servers (Orthanc) and now archives (dcm4che). Any healthcare organisation that has treated these as isolated vendor issues should reframe them as sustained security research attention on DICOM implementations generally, and should expect more. Second, the BeyondTrust zero-day in Priority Action 1 is a medical device security issue as much as an IT one: where a BeyondTrust appliance provides the remote-access route used by medical device vendors for maintenance, a compromised appliance gives an attacker that same path into the clinical estate. Biomedical engineering should be asked to confirm which vendor maintenance paths traverse BeyondTrust infrastructure, and whether those appliances are operated by you or by the vendor.

Threat Metrics

Activity Trends	Key Numbers This Week
▲ Remote-support appliances as the nation-state entry point: a second critical BeyondTrust flaw, zero-day exploited for seven weeks ▲ Medical device advisory cadence resumes: two new ICSMAs on one day, including a CRITICAL DICOM archive flaw ▲ Managed service provider trust relationships under direct attack via compromised service principals ▲ Autonomous AI offensive tooling: second such capability reported in four weeks ▲ Living-off-the-land breadth expanding — finger.exe now used as a payload downloader ▶ MeshAgent and ScreenConnect abuse continues — third consecutive week of legitimate RMM as the persistence layer	7 weeks — the gap between first observed exploitation of CVE-2026-102764 (Aug 29) and public disclosure (Oct 15) 3 days — CISA's federal remediation window for CVE-2026-102764, with forensic triage marked required 9.1 CVSS v3.1 CRITICAL — J4Care dcm4che, network reachable with no privileges and no user interaction 6 — distinct DICOM product lines now carrying CISA advisories in the current run 117 ATT&CK techniques mapped to GLOBAL.26.014 (ARTEX), the highest count recorded in this series 87 new GTI-verified IOCs; CVE-2026-3650 (GDCM): NO PATCH — week 30

Sources: Google Threat Intelligence (GTI) and Mandiant, CISA Alert — CISA Urges Patching Critical Vulnerability in BeyondTrust Remote Support (October 16, 2026), CISA Alert — CISA Adds Two Known Exploited Vulnerabilities to Catalog (October 16, 2026), CISA KEV Catalog, BeyondTrust Security Advisory BT26-05, CISA ICS Medical Advisories ICSMA-26-288-01 and -288-02 (October 15, 2026) plus -253-01, -253-02, -225-01, -223-01, -223-02, -218-01, -216-01, -181-01, -176-01, -176-02, -083-01, CISA ICS Medical Advisory index, Citrix Security Bulletin CTX697096, Joint Cybersecurity Advisories AA25-071A, AA26-222A, AA26-231A, AA26-237A, Rapid7, watchTower, SecurityWeek, Security Boulevard, Cyber Daily, NVD / CVE Program / MITRE, J4Care, Thermo Fisher Scientific, NextGen Healthcare, Orthanc