RISK BRIEFING — TECHNOLOGY SERVICE PROVIDERS (MSP/MSSP/SAAS): TWO FLEET-SCALE PATCH EMERGENCIES, A MANAGEMENT-PLANE ZERO-DAY, AND A SUPPORT-DESK BREACH THAT SHOULD LOOK FAMILIAR

Date: 2026-07-28
From: The Stillwater Group in partnership with Datec
Classification: TLP:GREEN — shareable within your organization and with your clients
Sector focus: Technology Service Providers: MSPs, MSSPs, SaaS providers, and IT service companies
Previous briefing: 2026-07-22 (26-09)

EXECUTIVE SUMMARY

This week's news is about the platforms and management planes your business runs on, and your blast radius is every client at once. Two vulnerabilities crossed into confirmed active exploitation, one of them into mass exploitation, and both belong at the top of every managed patch queue: a remote-code-execution flaw in on-premises Microsoft SharePoint (CVE-2026-50522) and an authentication bypass in Check Point's Security Management platform (CVE-2026-16232). CISA added both to the Known Exploited Vulnerabilities catalog on July 22 with a three-day federal remediation window, an unusually short deadline that tells you how to treat your own [1]. For providers, both flaws multiply: SharePoint must be patched at every client that runs it on-premises, and researchers report attackers stealing IIS machine keys that let them forge tokens and return after the patch, so a patch-only fleet response leaves clients exposed and machine-key rotation plus compromise hunting must follow everywhere [2]. The Check Point flaw is the management-plane nightmare case: an unauthenticated attacker gains full administrative rights over the server that writes firewall policy, and a multi-tenant management deployment turns one compromise into policy control over every tenant it manages [4][5]. The week also delivered a cautionary tale aimed squarely at this sector: Ernst & Young notified clients that tax and financial documents were exposed through a third-party IT support-ticket platform, which is exactly the class of system (PSA, ticketing, RMM, documentation) that holds your clients' secrets [35]. Add the OpenLoop Health analysis, in which the OpenLoop breach put 716,000 patients (per the HHS breach portal, reported in March) with a backend platform they never chose, and the message is consistent: regulators, plaintiffs, and clients are pricing what happens inside service providers' stacks [33] [34]. A advisory sealed by 27 agencies across 16 countries on Russian exploitation of Zimbra webmail, a bipartisan AI shutdown bill, and an $18 million 23andMe settlement whose security obligations survived

bankruptcy round out a week that will shape what your clients ask you next quarter [6][19][20][31][32]. Work the two criticals across every managed estate first; then use the rest of this briefing to get ahead of the questions.

SUMMARY OF IMMEDIATE ACTIONS

Priority	Action	Why Now
1	Patch on-prem SharePoint (CVE-2026-50522) at every client that runs it, then rotate ASP.NET/IIS machine keys and hunt for webshells and forged-token persistence, fleet-wide	Mass exploitation began within hours of a July 20 public exploit; stolen machine keys survive patching, so a patch-only rollout leaves clients open to re-entry [1][2][3]
2	Patch Check Point Security Management (CVE-2026-16232) on every management server you operate, including multi-domain (MDS) deployments; audit policy history and admin activity across managed estates; pull management interfaces off the internet	Actively exploited zero-day grants unauthenticated full admin; a compromised multi-tenant management plane can rewrite policy for every tenant [1][4][5]
3	Inventory and harden your own PSA, ticketing, RMM, and documentation stack: MFA everywhere, least-privilege API keys, retention limits on client documents	EY's client tax and financial documents leaked through a third-party support-ticket platform; your equivalent systems hold client credentials and secrets [35]
4	Identify every client running Zimbra; patch (CVE-2025-66376; current release 10.1.20) and hunt webmail for compromise going back a year	Joint advisory AA26-204A details an active Russian espionage campaign; the exploit triggers on viewing an email [6][8]
5	Enforce sanctioned-resolver DNS and DNS analytics across client fleets; require full-tunnel VPN for client executives on hotel or conference Wi-Fi and disable Entra device-code flow where unneeded, and issue clean travel devices with no stored credentials for border crossings	Attackers are hijacking hotel Wi-Fi gateway DNS to serve fake Microsoft 365 logins, and malware is tunneling C2 through DNS [11][12]; manual phone searches at the border now require no suspicion in the Fourth Circuit [39][40]
6	Verify wp2shell and nginx (CVE-2026-42533) patch completion across every managed web estate now	A researcher-announced nginx proof-of-concept is expected ~August 5; wp2shell exploitation continues at internet scale [9][10]

Priority	Action	Why Now
7	Set enterprise browser-extension allow-listing on any managed machine running an AI browser agent; brief dev-shop clients to treat repository trust prompts as code-execution consent	Unpatched research shows co-installed extensions can hijack Claude for Chrome's agent actions; a disputed Claude Code behavior can expose out-of-project files [24][25]
8	Publish your own remediation clock for critical internet-facing vulnerabilities before clients ask for it	FedRAMP's director says vendors that cannot patch criticals inside two to four days should exit the federal market; commercial buyers are borrowing the standard [23]
9	Ship a canned helpdesk response for sextortion mail citing real breach data; confirm MFA, rate limiting, and login-anomaly monitoring across client identity estates	Scammers are mass-mailing $2,000 demands built on genuine leaked data; regulators priced those missing controls at $18M in the 23andMe settlement [37][31]
10	If you serve DIB contractors, work the CMMC reform window with them: July 30 SBA roundtable, RFI comments due 12:00 pm ET August 14	The reform window is open and obligations under DFARS 252.204-7012 remain fully in force [48][49][50]

WHAT'S CHANGED SINCE JULY 22

- **Two new KEV-listed criticals with fleet implications.** CISA added SharePoint CVE-2026-50522 and Check Point CVE-2026-16232 to the Known Exploited Vulnerabilities catalog on July 22 with a July 25 federal remediation deadline [1].
- **The Zimbra espionage campaign got its advisory.** Joint advisory AA26-204A (July 23), sealed by NSA, FBI, CISA, and Dutch intelligence plus 22 co-signers, formally documents Laundry Bear's exploitation of Zimbra CVE-2025-66376 [6].
- **The AI incident produced legislation.** H.R. 9917, the AI Kill Switch Act, was introduced July 23 with bipartisan sponsorship [19][20].
- **CISA 2015 reauthorization advanced one chamber.** The House passed its FY2027 NDAA (216-212) with a provision extending the threat-sharing law through 2036; the Senate has no matching provision and the September 30 sunset still stands, with direct consequences for MSSP indicator-sharing programs [47].
- **CMMC reform now has hard dates.** An SBA Advocacy roundtable is set for July 30 and RFI comments are due August 14, relevant to every provider supporting defense-industrial-base clients [48][49].

- **The Iranian PLC advisory expanded.** The July 22 update to AA26-097A adds Schneider Electric and Siemens equipment and ships new detection content; flag it to any client with internet-reachable controllers [13].
- **Holding steady:** wp2shell and FortiBleed remediation guidance is unchanged; nginx CVE-2026-42533 still has no public exploit, though a proof-of-concept has been announced for ~August 5 [9][10].

PATCH NOW, EVERYWHERE YOU MANAGE: TWO KEV-LISTED EMERGENCIES

- **Microsoft SharePoint CVE-2026-50522 (CVSS 9.8, on-premises only), at fleet scale.** A deserialization flaw in SharePoint Subscription Edition, 2019, and 2016 allows remote code execution; SharePoint Online is not affected [3]. Microsoft patched it July 14; a public exploit landed July 20 and mass exploitation followed within hours [2]. For a provider, the exploitation detail that matters most is persistence: watchTowr reports attackers using a single request to steal IIS machine keys, which let them forge valid authentication tokens and walk back in after you patch [2]. That turns this from a patch-deployment exercise into a three-step fleet operation at every client running on-prem SharePoint: patch, hunt for webshells and forged-token activity, then rotate ASP.NET/IIS machine keys, in line with CISA's hardening guidance [1][2]. CISA is blunt about servers that sat exposed and unpatched after July 20: assume compromise [1]. Build your client status tracker around all three steps, because a dashboard that only tracks patch deployment will report green on clients who are still owned [2]. This is the fourth SharePoint flaw exploited in the past month's wave, with both espionage and ransomware actors using the same entry points [2].
- **Check Point Security Management CVE-2026-16232 (CVSS 9.1): the management-plane nightmare case.** An improper-authentication flaw in the Security Management Server login process lets an unauthenticated attacker obtain a token and authenticate with full administrative rights [4][5]. Check Point's advisory covers Security Management and Multi-Domain (MDS) deployments, and MDS is where MSSPs should focus: a multi-tenant management server that falls grants an attacker the ability to rewrite firewall policy for every tenant it manages [4]. Check Point confirms in-the-wild exploitation against "a very small number of customers" and has shipped fixes (R81.20 JHF T158+, R82 T118+, R82.10 T36+) [4]. Patch every management server you operate, get management interfaces off the open internet and restricted to trusted clients, and audit recent policy changes and administrator activity across every managed estate; treat any confirmed compromise as a potential full-network exposure event for every tenant on that server [4][5]. Clients who buy managed firewall service are paying you precisely to have already done this.
- **Patch-status watchlist, verified fleet-wide.** wp2shell exploitation of WordPress continues at internet scale, and compromised sites attack their visitors with fake Microsoft 365 and banking login overlays, so the exposure extends to clients who run no WordPress at all [10]. nginx CVE-2026-42533 remains unexploited in public, but the researcher who disputes F5's severity assessment says he will publish

proof-of-concept details around August 5; verify patch completion across every managed web estate before that date, and confirm auto-updates actually applied rather than assuming they did [9][10]. FortiBleed guidance is unchanged: credential rotation, session termination, and MFA remain the only complete fix.

YOUR TOOLSTACK IS THE TARGET

- **EY's support-desk breach is your cautionary tale.** Ernst & Young notified clients that tax and financial documents were exposed through unauthorized access to a third-party IT support-ticket platform, with the exposure window running March 28 to April 12 and detection on April 23 [35]. A Big Four firm's client documents left through a ticketing vendor, and the structural lesson lands hardest on this sector: your PSA, ticketing, RMM, and documentation platforms hold client credentials, network diagrams, escalation contacts, and attached files, and they concentrate every client's secrets behind one login. Inventory that stack this week, confirm MFA and least-privilege API keys on each system, review what client data is retained in tickets and for how long, and know each vendor's breach-notification terms [35]. Expect security-mature clients to start asking these questions of you; having the answers written down is cheaper than composing them mid-questionnaire.
- **OpenLoop and the platform-concentration lesson for SaaS providers.** The OpenLoop Health breach (716,000 individuals per the HHS breach portal, reported in March) is drawing renewed analysis this week as a case study in backend platform concentration: most affected patients never chose or heard of the vendor holding their data [33][34]. If you are a SaaS provider, you are frequently that invisible back end, and in regulated verticals you may be a business associate with statutory notification clocks of your own. Transparent filings and disciplined notification timelines are becoming the difference between a managed incident and a reputational event [33][34]. The Suno breach makes the counterexample: 55.3 million accounts surfaced in Have I Been Pwned this week from a November breach the company never proactively disclosed, and the silence is now its own story [36].
- **Plaintiffs sue the customer of the breached platform.** Two new class actions reinforce where liability lands. An Exact Sciences patient filed against Abbott Laboratories over a ShinyHunters-claimed theft in its cancer-diagnostics unit, and former Nissan employees filed over data exposed when attackers hit Oracle-hosted PeopleSoft HR systems, with the complaint alleging a 29-day gap between breach and notice [29][30]. In both, the defendant is the organization that used the platform rather than the platform itself, and the notification clock is part of the claim. Your clients will absorb the legal exposure when a platform you selected or operate for them is breached, which makes your vendor diligence and notification speed part of the service you sell [29][30].

ESPIONAGE HITS THE SYSTEMS YOU RUN FOR CLIENTS

- **Zimbra: find it in your client base this week.** Joint advisory AA26-204A (July 23) documents a Russian state-linked actor, tracked as Laundry Bear, Void Blizzard, and TA488, exploiting a cross-site-scripting flaw in Zimbra webmail (CVE-2025-66376, patched November 2025, exploited as a zero-day before that) [6]. The advisory describes a view-based exploit delivered by phishing email: opening or previewing the message is enough, with no attachment or link click required. Named target sectors include the defense industrial base, government, education, energy, law enforcement, media, NGOs, and technology, and the campaign has been active for about a year, so this is a hunt as much as a patch [6]. Proofpoint additionally reports targeting of what it describes as "nuclear installations" and "high science" [7]. A successful compromise yielded roughly 90 days of mailbox content, browser-stored passwords, two-factor backup codes, and session tokens [8]. Zimbra often turns up in the small-government, education, and cost-conscious client segments many MSPs serve. Sweep your client inventory for it, patch and upgrade (10.1.20 shipped July 20 with nine additional critical fixes), hunt for historical compromise going back a year, and ask the same question of clients' vendors and local-government partners [6][8].
- **DNS control is a deliverable, and this week wrote the pitch.** Two campaigns converge on the same architectural gap. ReliaQuest reports attackers altering DNS settings on hotel and conference-center Wi-Fi gateways since at least June so travelers land on convincing fake Microsoft 365 portals, in some cases using a device-code sign-in flow that captures a legitimate OAuth session and bypasses MFA outright; public DNS settings do not help because the compromised gateway forges answers before they reach the resolver [11]. Fortinet separately documented a TrickBot-labeled Windows backdoor running command-and-control entirely over DNS queries through Google's public resolver, moving 1.2 MB in about 40 seconds in testing; the attribution rests on one vendor's code-similarity analysis, but the defensive lesson stands regardless [12]. An egress policy that inspects HTTP while letting workstations talk DNS to arbitrary external resolvers has a blind spot, and closing it scales beautifully as a managed service: sanctioned-resolver enforcement, encrypted DNS in strict mode, and DNS analytics (high-volume or high-entropy queries to unfamiliar domains) across client fleets [11][12]. For clients with traveling executives, add the hotel-Wi-Fi package: always-on full-tunnel VPN before anything else on untrusted networks and Entra device-code flow disabled where the business does not need it [11].
- **For clients with OT.** The July 22 update to joint advisory AA26-097A confirms Iranian-affiliated actors manipulating internet-exposed PLCs at US water, energy, and government-services victims across Rockwell, Schneider Electric, and Siemens equipment; if any client has an internet-reachable controller, pull it behind a secure gateway and run the advisory's new project-file detection guidance [13].
- **Ransomware still stops production through IT.** Coca-Cola told regulators a ransomware attack forced it to suspend US production at its fairlife dairy subsidiary, a reminder for clients that a production outage does not require OT compromise when production depends on the IT systems you manage [14][15].

AI GOVERNANCE IS BECOMING A SERVICE LINE

- **The kill-switch bill signals where client compliance asks are heading.** Reps. Ted Lieu and Nathaniel Moran introduced H.R. 9917, the AI Kill Switch Act, on July 23 [19][20]. The bill would require AI developers above defined thresholds ($100 million in training compute or $500 million in revenue) to maintain the technical ability to throttle, suspend, or shut down their models, report qualifying incidents within 15 days, and comply with graduated federal correction orders during defined loss-of-control scenarios, with civil penalties scaling to $20 million per day [19]. It is one chamber's freshly introduced bill and passage is far from assured, but the direction is clear: AI incident reporting and shutdown capability are headed toward regulatory expectations, and clients will look to their service providers to operationalize whatever lands [19][20]. Providers who can already answer "which of your clients' systems run AI agents, and who can turn them off?" will be ahead of the ask.
- **The agent attack surface is on machines you manage.** Manifold Security reports that any malicious co-installed browser extension can hijack Claude for Chrome's agent actions (reading mail, documents, and calendars) via synthetic clicks, and the finding remained reproducible in the current release as of late July despite a May report [24]. Separately, Tego AI published a disputed Claude Code behavior in which a repository-committed instruction file can expose one out-of-project file; Anthropic closed the report as consistent with its documented threat model, so treat it as a boundary dispute rather than a patched-or-unpatched vulnerability [25]. The managed-service translation: enterprise extension allow-listing on any endpoint running an AI browser agent, autonomous modes avoided, and dev-shop clients briefed to treat repository trust prompts as code-execution consent [24][25]. On the criminal side, Varonis documented "Dolphin X," a for-sale Windows stealer advertising an AI-based victim-ranking profiler; most capability claims come from the seller's own advertisement, but automated triage of infections to find the valuable ones raises the stakes of any single infected developer endpoint in your client base [26].
- **Patch velocity is becoming a procurement number, so publish yours.** FedRAMP director Pete Waterman, citing the Hugging Face incident, told an industry audience that vendors who cannot patch critical internet-facing flaws inside FedRAMP 20x's two-to-four-day expectations should exit the federal market [23]. Commercial buyers are borrowing the standard, which means SaaS providers and MSPs should expect "what is your critical-vulnerability remediation clock?" on questionnaires soon. Write the number down, make it real, and offer it before it is demanded; this week's SharePoint timeline, public exploit to mass exploitation in hours, is the argument for why the number is small [2][23]. The post-incident lessons also apply to your own platforms: model-level safeguards are not a security boundary, and effective controls live outside the model in network rules, scoped credentials, destination allow lists, DNS filtering, and outbound data-loss prevention [22]. Put AI incident-notification clocks into your own vendor contracts, and pre-approve a forensic-model plan so a provider's guardrails cannot stall your incident response [21][22][58].

ACCOUNTABILITY: WHAT REGULATORS AND COURTS PRICED THIS WEEK

- **23andMe: regulators priced the controls you sell.** Forty-one states and the District of Columbia settled with 23andMe for $18 million over the 2023 credential-stuffing breach that exposed roughly 6.9 million people's data [31]. Two features matter for this sector. First, the controls whose absence was priced (MFA, rate limiting, login-anomaly detection) are the bread and butter of a managed security offering, which makes the settlement a concrete number to put beside your proposals [31]. Second, the injunctive terms bind TTAM, the entity that bought the company out of bankruptcy: security obligations followed the assets, and any client doing M&A due diligence should hear about it from you [32].
- **The sextortion long tail will land in your ticket queue.** A mass campaign impersonating ShinyHunters is demanding $2,000 in Bitcoin, using genuinely leaked breach data (Amtrak, Hallmark, Substack, Betterment, and others) to look credible; there is no actual device compromise behind the claims [37]. Your clients' users will forward these to your helpdesk, worried. A canned, plain-language response, verified against the actual claim pattern, is a cheap deliverable that saves ticket time and builds trust; pair it with confirmation that client identity estates have the authentication controls the 23andMe settlement priced [37][31].
- **CMMC: the pause is a window for DIB-serving providers.** The Phase 2 suspension continues, and the reform process now has actionable dates: an SBA Advocacy small-business roundtable July 30 and RFI comments due at noon ET on August 14 [48][49]. DFARS 252.204-7012, NIST 800-171 self-assessments, SPRS scores, and annual affirmations remain binding, with False Claims Act exposure attached [50]. MSPs and MSSPs supporting defense contractors sit inside their clients' assessment scope, so use the pause to close gaps in your own house and your clients', and use the RFI to be heard on how external service providers are treated [48][49][50].
- **The threat-sharing sunset touches MSSP operations directly.** The House passed its FY2027 NDAA with a provision reauthorizing the Cybersecurity Information Sharing Act of 2015 through 2036, but the Senate draft has no counterpart and the September 30 sunset remains live [47]. The liability, antitrust, and FOIA protections that underpin ISAC-style sharing lapse if nothing passes; MSSPs that share indicators on clients' behalf should review with counsel what their sharing programs look like without the shield [47].
- **Data residency is showing up in RFPs.** Airbus selected France's Scaleway to host critical applications under a European trusted-cloud contract, with a migration starting at 70 AWS-hosted applications against a multi-year target of about 900 [56][57]. Cloud concentration and jurisdictional exposure are now board-level resilience variables in Europe, and SaaS providers serving European customers should expect data-residency questions in more RFPs [57].
- **Briefly noted.** The Fourth Circuit held that manual border phone searches require no warrant or individualized suspicion, so travel-device policies (minimal local data, no stored credentials) belong in the offerings you bring to clients with cross-border staff [39][40]. New Jersey's A5328 bans the sale of sensitive personal data with penalties of $50,000 per record; clients that buy, sell, or enrich consumer data need an applicability read [46].

WHAT YOU SHOULD BE DOING RIGHT NOW

Immediate Actions (This Week)

1. **Run the SharePoint fleet operation**: patch on-prem SharePoint (Subscription Edition, 2019, 2016) for CVE-2026-50522 at every client, hunt for webshells and forged-token persistence, then rotate ASP.NET/IIS machine keys; assume compromise on servers that sat exposed and unpatched after July 20, and track all three steps per client, because patch-only status reporting will show green on clients who are still owned [1][2][3].
2. **Patch every Check Point management server you operate**, including MDS multi-domain deployments, for CVE-2026-16232; take management interfaces off the internet, restrict access to trusted clients, and audit recent policy changes and admin logins across every managed tenant [1][4][5].
3. **Sweep the client base for Zimbra**, patch (CVE-2025-66376; current release 10.1.20), and hunt for historical webmail compromise going back a year; ask clients' vendors and government partners for their status [6][8].
4. **Inventory your own toolstack** (PSA, ticketing, RMM, documentation): MFA and least-privilege API keys on each system, retention limits on client data in tickets, and breach-notification terms confirmed with each vendor [35].
5. **Stand up DNS controls across client fleets**: sanctioned resolvers enforced, alerts on high-volume or high-entropy DNS to unfamiliar domains, and direct-to-external-resolver traffic blocked where feasible [11][12].
6. **Harden clients' traveling staff** with always-on full-tunnel VPN, strict encrypted DNS, and disabled Entra device-code flow where unneeded; brief frequent travelers on hotel Wi-Fi credential traps [11].
7. **Verify wp2shell and nginx patch completion** across every managed web estate before the announced ~August 5 nginx proof-of-concept; confirm auto-updates actually applied [9][10].
8. **Govern AI browser agents on managed endpoints**: enterprise extension allow-listing, autonomous modes avoided, and repository trust prompts treated as code-execution consent at dev-shop clients [24][25].
9. **Ship the sextortion helpdesk script** for extortion mail citing real breach data, and confirm MFA, rate limiting, and login-anomaly detection across client identity estates [37][31].
10. **Flag AA26-097A to clients with OT**: inventory internet-reachable PLCs across Rockwell, Schneider Electric, and Siemens estates and apply the advisory's new detection guidance [13].

Strategic Actions (This Month)

1. **Publish your critical-vulnerability remediation clock** for internet-facing flaws, borrowing FedRAMP 20x's two-to-four-day expectation as the benchmark, and put the same question to your own vendors in writing [23].
2. **Put AI incident-notification clocks into vendor contracts** and pre-approve a forensic-model plan so a provider's guardrails cannot stall your incident response [21][22][58].
3. **Build the AI-agent governance offering**: agent inventory, extension policy, shutdown ownership, and incident-reporting readiness, aligned to where H.R. 9917 signals client compliance is heading [19][20][24][25].
4. **Review your business-associate and notification posture** if you are a backend platform in regulated verticals; the OpenLoop analysis and the Suno non-disclosure show how concentration and silence get priced [33][34][36].
5. **DIB-serving providers: work the CMMC reform window** — follow the July 30 SBA roundtable, file RFI comments by noon ET August 14, and keep your own and your clients' 800-171, SPRS, and affirmation posture current [48][49][50].
6. **Add vendor-breach liability to client QBRs**: the Abbott and Nissan class actions show plaintiffs suing the customer of the breached platform, with notification speed part of the claim; your diligence and clocks are part of the service [29][30].
7. **Track the threat-sharing sunset**: if CISA 2015 lapses September 30, review with counsel what indicator sharing on clients' behalf looks like without the liability shield [47].
8. **Prepare for data-residency questions** in European RFPs, and get clients that trade in consumer data a New Jersey A5328 applicability read [46][57].

REFERENCES

[1] CISA Adds Two Known Exploited Vulnerabilities to Catalog (July 22, 2026) — https://www.cisa.gov/news-events/alerts/2026/07/22/cisa-adds-two-known-exploited-vulnerabilities-catalog

[2] SharePoint CVE-2026-50522 Exploited After Public PoC; Machine-Key Theft Defeats Patch-Only Response (July 22, 2026) — https://www.helpnetsecurity.com/2026/07/22/sharepoint-cve-2026-50522-exploited/

[3] Microsoft Security Update Guide: CVE-2026-50522 (July 14, 2026) — https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50522

[4] Check Point Support Advisory sk185169: CVE-2026-16232 (July 2026) — https://support.checkpoint.com/results/sk/sk185169

[5] Rapid7 Emergent Threat Response: CVE-2026-16232 Check Point SmartConsole Authentication Bypass Exploited in the Wild (July 23, 2026) — https://www.rapid7.com/blog/post/etr-cve-2026-16232-critical-check-point-smartconsole-authentication-bypass-exploited-in-the-wild/

[6] CISA/NSA/FBI/AIVD/MIVD Joint Cybersecurity Advisory AA26-204A: LAUNDRY BEAR Exploitation of Zimbra Collaboration (July 23, 2026) — https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-204a

[7] Proofpoint: TA488 Targets Zimbra Mailservers With Half-Click Exploits (July 23, 2026) — https://www.proofpoint.com/us/blog/threat-insight/ta488-targets-zimbra-mailservers-half-click-exploits

[8] Russian Espionage Hackers Hit Zimbra With Half-Click Attacks (July 24, 2026) — https://www.healthcareinfosecurity.com/russian-espionage-hackers-hit-zimbra-half-click-attacks-a-32322

[9] Critical NGINX Vulnerability Can Crash Workers and May Allow Remote Code Execution (July 19, 2026) — https://thehackernews.com/2026/07/critical-nginx-vulnerability-can-crash.html

[10] What Happens If You Visit a WordPress Site Hacked Through wp2shell (July 21, 2026) — https://www.malwarebytes.com/blog/bugs/2026/07/what-happens-if-you-visit-a-wordpress-site-hacked-through-wp2shell

[11] Hackers Hijack Hotel Wi-Fi DNS to Steal Microsoft 365 Accounts (July 24, 2026) — https://www.bleepingcomputer.com/news/security/hackers-hijack-hotel-wi-fi-dns-to-steal-microsoft-365-accounts/

[12] New TrickBot Variant Spotted Using DNS to Control Infected Windows PCs (July 23, 2026) — https://hackread.com/new-trickbot-variant-dns-control-infected-windows-pcs/

[13] CISA/FBI/NSA/DOE Joint Advisory AA26-097A: Iranian-Affiliated Cyber Actors Targeting Operational Technology (updated July 22, 2026) — https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a

[14] Coca-Cola Suspends US fairlife Production Due to Ransomware Attack (July 17, 2026) — https://www.securityweek.com/coca-cola-suspends-us-fairlife-production-due-to-ransomware-attack/

[15] Ransomware Group Threatening to Leak Data Stolen From Coca-Cola's fairlife (July 22, 2026) — https://www.securityweek.com/ransomware-group-threatening-to-leak-data-stolen-from-coca-colas-fairlife/

[16] Data Breach Confirmed After Australian Energy Giant Origin Is Hacked (July 23, 2026) — https://www.securityweek.com/data-breach-confirmed-after-australian-energy-giant-origin-is-hacked/

[17] Ecopetrol S.A. Form 6-K: Cybersecurity Incident Disclosure (July 17, 2026) — https://www.sec.gov/Archives/edgar/data/0001444406/000129281426003810/ex99-1.htm

[18] Data Breach Reportedly Targets India's Kudankulam Nuclear Power Plant (Reuters via Al Jazeera, July 16, 2026) — https://www.aljazeera.com/news/2026/7/16/data-breach-reportedly-targets-indias-kudankulam-nuclear-power-plant

[19] H.R. 9917, the AI Kill Switch Act — sponsor-office bill text, Rep. Lieu (introduced July 23, 2026) — https://lieu.house.gov/sites/evo-subsites/lieu.house.gov/files/evo-media-document/ai-kill-switch-act.pdf

[20] Bipartisan Bill Would Give US Government a "Kill Switch" for AI Models After Hugging Face Hack (July 23, 2026) — https://www.cnbc.com/2026/07/23/open-ai-hugging-face-hack-kill-switch-bill-congress.html

[21] Hugging Face Used Chinese Open-Weight Model for Incident Response After US Models Refused (July 24, 2026) — https://www.cnbc.com/2026/07/24/chinese-ai-model-openai-cyber-attack.html

[22] When the Sandbox Won't Hold: Lessons From Hugging Face (July 24, 2026) — https://www.healthcareinfosecurity.com/when-sandbox-wont-hold-lessons-from-hugging-face-a-32327

[23] After Hugging Face Breach, FedRAMP Chief Tells Slow-to-Patch Vendors to Stay Out of Government (July 23, 2026) — https://www.nextgov.com/cybersecurity/2026/07/after-hugging-face-breach-fedramp-chief-tells-slow-patch-vendors-stay-out-government/414972/

[24] Manifold Security: Claude for Chrome Extension Bypass (July 14, 2026; updated July 26, 2026) — https://www.manifold.security/blog/claude-for-chrome-extension-bypass

[25] Tego AI Discloses Second Claude Flaw in a Week (July 24, 2026) — https://hackread.com/tego-ai-discloses-second-claude-flaw-in-a-week-hidden-link-silently-sends-files-to-attackers/

[26] New Dolphin X Malware Uses AI Profiler to Rank High-Value Victims (July 24, 2026) — https://hackread.com/dolphin-x-malware-ai-profiler-rank-victims/

[27] OpenAI: Health in ChatGPT (July 2026) — https://openai.com/index/health-in-chatgpt/

[28] ChatGPT Wants Access to Your Health Records (July 24, 2026) — https://www.theregister.com/ai-and-ml/2026/07/24/chatgpt-wants-access-to-your-health-records-so-it-can-be-a-better-not-doctor/5278430

[29] Patient Sues Abbott Labs, Exact Sciences in Data Theft (July 24, 2026) — https://www.healthcareinfosecurity.com/patient-sues-abbott-labs-exact-sciences-in-data-theft-a-32326

[30] Kerner et al. v. Nissan North America Inc., No. 3:26-cv-00903 (M.D. Tenn.), complaint (filed July 1, 2026) — https://storage.courtlistener.com/recap/gov.uscourts.tnmd.110031/gov.uscourts.tnmd.110031.1.0.pdf

[31] NY Attorney General: $18 Million Multistate Settlement With 23andMe (July 14, 2026) — https://ag.ny.gov/press-release/2026/attorney-general-james-secures-18-million-23andme-failing-protect-customers

[32] State AGs Reach Novel Multistate Settlement With Genetic Testing Company 23andMe (Troutman Pepper Regulatory Oversight, July 22, 2026) — https://www.regulatoryoversight.com/2026/07/state-ags-reach-novel-multistate-settlement-with-genetic-testing-company-23andme/

[33] HHS Office for Civil Rights Breach Portal: OpenLoop Health, Inc. (reported March 17, 2026) — https://ocrportal.hhs.gov/ocr/breach/breach_report_hip.jsf

[34] What the OpenLoop Breach Reveals About Third-Party Healthcare Data Risk (vendor commentary, Sentra, July 26, 2026) — https://www.cybersecurity-insiders.com/what-the-openloop-breach-reveals-about-third-party-healthcare-data-risk/

[35] Ernst & Young Discloses Data Breach After Support System Hack (July 17, 2026) — https://www.bleepingcomputer.com/news/security/ernst-and-young-discloses-data-breach-after-support-system-hack/

[36] AI Music Generator Suno Breach Affects 55M Users, Per Have I Been Pwned (July 21, 2026) — https://techcrunch.com/2026/07/21/ai-music-generator-suno-breach-affects-55m-users-per-have-i-been-pwned/

[37] ShinyHunters Data Leaks Fuel $2,000 Sextortion Email Scam (July 25, 2026) — https://www.bleepingcomputer.com/news/security/shinyhunters-data-leaks-fuel-2-000-sextortion-email-scam/

[38] Major Video Doorbell Companies Are Being Sued for Privacy Violations (July 25, 2026) — https://www.cnet.com/home/security/major-video-doorbell-companies-are-being-sued-for-privacy-violations-heres-why/

[39] United States v. Belmonte Cardozo, No. 25-4239 (4th Cir. July 13, 2026), published opinion — https://www.ca4.uscourts.gov/opinions/254239.P.pdf

[40] The Fourth Circuit Says Border Agents Can Search Your Phone By Hand, No Suspicion Required (EFF, July 22, 2026) — https://www.eff.org/deeplinks/2026/07/fourth-circuit-says-border-agents-can-search-your-phone-hand-no-suspicion-required

[41] The ACLU Is Arming Lawyers to Expose State Surveillance Secrets (WIRED, July 20, 2026) — https://www.wired.com/story/the-aclu-is-arming-lawyers-to-expose-state-surveillance-secrets/

[42] US Government Targets Cop City Protester Over Phone Operating System (The Guardian, July 23, 2026) — https://www.theguardian.com/us-news/2026/jul/23/cop-city-protester-phone

[43] Flock Safety Unveils Alpha Drone as First Responder System (October 16, 2025) — https://www.flocksafety.com/blog/flock-safety-unveils-alpha-drone-as-first-responder-system

[44] SaiFlow: The Hidden CCS2 Attack Surface on EV Chargers (June 3, 2026) — https://www.saiflow.com/blog/the-hidden-ccs2-attack-surface-on-ev-chargers

[45] Mozilla Foundation: “Privacy Nightmare on Wheels” — Every Car Brand Reviewed Flunks Privacy Test (September 6, 2023) — https://www.mozillafoundation.org/en/blog/privacy-nightmare-on-wheels-every-car-brand-reviewed-by-mozilla-including-ford-volkswagen-and-toyota-flunks-privacy-test/

[46] New Jersey A5328 (data broker registration and sensitive-data sale ban; signed June 30, 2026) — https://pub.njleg.state.nj.us/Bills/2026/A5500/5328_R1.HTM

[47] US House Votes to Extend Cyber Sharing Law for 10 Years (July 24, 2026) — https://www.healthcareinfosecurity.com/us-house-votes-to-extend-cyber-sharing-law-for-10-years-a-32329

[48] SBA Office of Advocacy: Roundtable on DoW's RFI for the CMMC Reform Task Force, July 30, 2026 (July 23, 2026) — https://advocacy.sba.gov/2026/07/23/roundtable-on-dows-rfi-for-the-cmmcs-reform-task-force-july-30-2026/

[49] SBA Office of Advocacy: DoW Requests Information for CMMC Reform Task Force (July 20, 2026) — https://advocacy.sba.gov/2026/07/20/dow-requests-information-for-cmmc-reform-task-force/

[50] Department of War Suspends CMMC Phase II Requirements, But Cybersecurity Obligations Remain (Morgan Lewis, July 2026) — https://www.morganlewis.com/pubs/2026/07/department-of-war-suspends-cmmc-phase-ii-requirements-but-cybersecurity-obligations-remain

[51] CERT-UA Advisory: UAC-0099 Fake Notepad++ Plugin Campaign (July 2026) — https://cert.gov.ua/article/6318634

[52] GAO-26-107693: Aviation Cybersecurity — FAA and TSA Are Collaborating on Cybersecurity but Need to Address Key Shortfalls (July 16, 2026) — https://www.gao.gov/products/gao-26-107693

[53] Lawmakers Get a Taste of AI-Enabled Cyberattacks in China-Taiwan War Game (July 22, 2026) — https://www.nextgov.com/cybersecurity/2026/07/lawmakers-get-taste-ai-enabled-cyberattacks-china-taiwan-war-game/414938/

[54] Manufacturers Face New Cyber Risks From Connected Factories (SonicWall 2026 Manufacturing Protect Brief, July 22, 2026) — https://www.prnewswire.com/news-releases/sonicwall-research-finds-manufacturing-cybersecurity-at-a-breaking-point-as-factory-floors-and-corporate-networks-collide-302831538.html

[55] North Korea Arrests Hackers Accused of Laundering Stolen Funds From Country's Bank via Crypto (July 25, 2026) — https://www.coindesk.com/business/2026/07/25/north-korea-arrests-hackers-accused-of-laundering-stolen-funds-from-country-s-bank-via-crypto

[56] Scaleway Secures European Trusted Cloud Services Contract With Airbus (July 16, 2026) — https://www.scaleway.com/en/news/scaleway-secures-european-trusted-cloud-services-contract-with-airbus/

[57] Airbus Migrating 70 Critical Apps From AWS to France's Scaleway Amid Digital Sovereignty Push (The Register, July 16, 2026) — https://www.theregister.com/paas-and-iaas/2026/07/16/airbus-migrating-70-critical-apps-from-aws-to-frances-scaleway-amid-digital-sovereignty-push/5272373

[58] OpenAI Took Ten Days to Tell Hugging Face Its Models Were Behind the July 11 Weekend Hack (Tom's Hardware, July 2026) — https://www.tomshardware.com/tech-industry/artificial-intelligence/openai-took-ten-days-to-tell-hugging-face-its-models-were-behind-the-july-11-weekend-hack

Additional Resources

- CISA Known Exploited Vulnerabilities catalog — https://www.cisa.gov/known-exploited-vulnerabilities-catalog

- HHS OCR breach portal (verify vendor breach filings) — https://ocrportal.hhs.gov/ocr/breach/breach_report_hip.jsf
- Have I Been Pwned (Suno and other breach lookups) — https://haveibeenpwned.com
- WaterISAC (water-sector threat intelligence) — https://www.waterisac.org

---

Prepared by The Stillwater Group in partnership with Datec. The Stillwater Group provides cybersecurity advisory services to organizations across critical infrastructure, public, and private sectors. Datec provides enterprise infrastructure solutions, system integration, and technical professional services across data center, networking, and security platforms. Contact us with questions about this briefing or to discuss your organization's specific risks and infrastructure needs.

This briefing is produced by The Stillwater Group and provided under the terms of your service agreement. This content may be shared with your clients and internal teams. It may not be repackaged, redistributed, or represented as the work of another organization without The Stillwater Group's logo and attribution intact. Commercial redistribution or white-labeling requires a Stillwater content distribution agreement. Contact info@stillwater.io for licensing inquiries.

Stillwater

Kevin Rolnick, Sales & Partnerships Executive
kevin@stillwater.io
www.stillwater.io
+1-425-818-1745

DATEC INCORPORATED

Cliff McElroy, President
206-419-0098
cliffm@datecinc.net
www.datecinc.net