RISK BRIEFING, CRITICAL INFRASTRUCTURE EDITION: PLC MANIPULATION WIDENS ACROSS VENDORS, ESPIONAGE REACHES LOCAL-GOVERNMENT MAIL, AND TWO PATCH-NOW EMERGENCIES

Date: 2026-07-28
From: The Stillwater Group in partnership with Datec
Classification: TLP:GREEN, shareable within your organization and with sector peers
Sector focus: Cities, public agencies, water and power districts, 911 PSAPs, utilities, transportation, and shipping
Previous briefing: 2026-07-22 (26-09)

EXECUTIVE SUMMARY

The most important item for this sector is the July 22 update to joint advisory AA26-097A: Iranian-affiliated actors have been manipulating internet-exposed programmable logic controllers at US water and wastewater, energy, and government-services victims since at least March, and the advisory now covers Schneider Electric and Siemens equipment in addition to Rockwell [13]. The actors exfiltrate PLC project files, alter or delete control logic, manipulate operator displays, and in at least one FBI-observed case installed a malicious project file that preserved normal downstream function while overriding safe-operating parameters; they have also disabled alarm and shutdown logic [13]. The update ships concrete detection guidance for malicious project-file changes, and this briefing translates it into a work plan for the week. Alongside that, two vulnerabilities crossed into confirmed active exploitation, one of them into mass exploitation, and belong at the top of every municipal and agency 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 an unusually short three-day federal remediation window [1]. A advisory sealed by 27 agencies across 16 countries on the Russian "Laundry Bear" espionage campaign against Zimbra webmail names federal and local government and energy among its target sectors, which puts many municipal and district IT shops directly in scope [6]. Ransomware halted US production at Coca-Cola's fairlife dairy subsidiary, a working example of critical-infrastructure impact in the food and agriculture sector, with the attackers' publication deadline landing the day after this briefing [14][15]. Utility customer-data estates took hits at Australia's Origin Energy and Colombia's Ecopetrol, a reminder that billing and CRM systems are a soft target distinct from grid OT [16][17]. Finally, with the 2026 election cycle underway, we give election-

infrastructure risk its own standing section: the legal protections underpinning threat-indicator sharing lapse September 30 absent Senate action, and election offices should verify their intelligence channels now rather than in October [47].

SUMMARY OF IMMEDIATE ACTIONS

Priority	Action	Why Now
1	Inventory every internet-reachable PLC across Rockwell, Schneider Electric, and Siemens estates, pull them behind secure gateways, and run AA26-097A's new project-file detection guidance	Iranian-affiliated actors are manipulating PLCs at US water, energy, and government-services victims and have disabled alarm and shutdown logic [13]
2	Patch on-prem SharePoint (CVE-2026-50522), then rotate ASP.NET/IIS machine keys and hunt for webshells and forged-token persistence	Mass exploitation began within hours of a July 20 public exploit; stolen machine keys survive patching [1][2][3]
3	Patch Check Point Security Management (CVE-2026-16232), take management interfaces off the internet, and audit recent firewall policy changes	Actively exploited zero-day grants unauthenticated full admin over the platform that writes your firewall policy [1][4][5]
4	Confirm Zimbra is patched for CVE-2025-66376 and current (10.1.20); hunt webmail for compromise and ask regional partners running Zimbra the same question	Joint advisory AA26-204A names federal and local government and energy among target sectors; the exploit triggers on viewing an email [6][8]
5	Election offices and their vendors: verify every election threat-sharing membership, indicator-sharing agreement, and peer channel is active and tested	The liability protections behind voluntary threat sharing lapse September 30 unless the Senate acts [47]
6	Rehearse ransomware production-impact and extortion-payment decisions with executives and counsel before you need them	Ransomware suspended US production at fairlife; Coca-Cola has confirmed data was taken, and the attackers posted the stolen data for download after their July 27 deadline passed [14][15][59][60]

Priority	Action	Why Now
7	Review customer-data estates (billing, CRM, payment systems) as a protection scope distinct from OT	Origin Energy confirmed customer-data access affecting a base of about 4.8 million customers; Ecopetrol disclosed cloud-storage access across roughly 15 subsidiaries [16][17]
8	Require full-tunnel VPN for traveling operations staff on hotel or conference Wi-Fi; disable Entra device-code flow where unneeded; restrict outbound DNS to sanctioned resolvers, 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 command-and-control through DNS [11][12]; manual phone searches at the border now require no suspicion in the Fourth Circuit [39][40]
9	Verify WordPress (wp2shell) and nginx (CVE-2026-42533) patch completion on public-facing municipal and utility sites	A researcher-announced nginx proof-of-concept is expected ~August 5; wp2shell exploitation continues at internet scale [9][10]
10	Map where facility design documents sit with EPC and engineering contractors, and in whose data centers	The Kudankulam leak traveled through a contractor's outsourced hosting, and the extortionists priced the end client's criticality [18]

WHAT'S CHANGED SINCE JULY 22

- **The Iranian PLC advisory expanded.** The July 22 update to AA26-097A adds Schneider Electric and Siemens equipment to the previously Rockwell-focused guidance and ships new detection content for malicious project-file changes [13].
- **Two new KEV-listed criticals.** 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, with local government and energy among named target sectors [6].
- **The fairlife data is out.** The Anubis ransomware group's publication deadline of Monday, July 27 passed, and the group has since posted the data it stole from Coca-Cola's dairy subsidiary for download; Coca-Cola has confirmed data was taken, though the claimed 1 TB volume remains the attackers' own figure [15][59][60].

- **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 [47].
- **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].

THE PLC CAMPAIGN: WHAT A UTILITY SHOULD DO THIS WEEK

The July 22 update to joint advisory AA26-097A (FBI, CISA, NSA, EPA, the Department of Energy, Cyber National Mission Force, and Treasury) is the operational center of gravity for this sector. It confirms that Iranian-affiliated actors who have been manipulating internet-exposed programmable logic controllers at US water, energy, and government-services victims since at least March are now observed on Schneider Electric and Siemens equipment in addition to Rockwell [13]. The observed tradecraft matters for defense: the actors exfiltrate PLC project files, alter or delete control logic, manipulate what operators see on their displays, and have disabled alarm and shutdown logic; in at least one FBI-observed case they installed a malicious project file that kept downstream processes looking normal while overriding safe-operating parameters [13]. The advisory attributes the activity to an unnamed Iranian-affiliated APT group and ships new detection guidance for malicious project-file changes [13].

A concrete work plan for the week, for a water or power district of any size:

1. **Inventory exposure.** Identify every controller, HMI, and OT gateway reachable from the internet, including cellular and serial modems; if any controller in your estate is internet-reachable, treat yourself as in scope regardless of vendor [13].
2. **Remove the exposure.** Pull exposed devices behind secure gateways or VPN; where a device must stay remotely reachable for operations, restrict it to known source addresses and require strong authentication [13].
3. **Run the detection guidance.** Apply the advisory's new project-file detection content, and compare running PLC logic against your engineering baselines, with specific attention to alarm setpoints and shutdown logic, since disabling those is observed behavior [13].
4. **Brief the control room.** Operators should know that manipulated displays are part of this campaign and should escalate any mismatch between displayed values and physical indications [13].
5. **Confirm manual fallback.** Verify you can run critical processes manually if control-system integrity comes into question, and that the people who know how are reachable.

PATCH NOW: TWO KEV-LISTED EMERGENCIES IN MUNICIPAL AND AGENCY FLEETS

- **Microsoft SharePoint CVE-2026-50522 (CVSS 9.8, on-premises only).** A deserialization flaw in SharePoint Subscription Edition, 2019, and 2016 allows remote code execution; SharePoint Online is not affected [3]. Many cities, districts, and agencies still run on-prem SharePoint for records, permitting, and intranet workloads, and those servers are squarely in scope. Microsoft patched it July 14; a public exploit landed July 20 and mass exploitation followed within hours [2]. The detail that matters most: researchers report 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]. CISA's hardening guidance is blunt: assume compromise on internet-exposed unpatched servers, hunt and remediate, then rotate machine keys [1] [2].
- **Check Point Security Management CVE-2026-16232 (CVSS 9.1).** An improper-authentication flaw in the Security Management Server login process lets an unauthenticated attacker obtain a token and authenticate with full administrative rights, which means the ability to rewrite firewall policy for everything the platform manages [4][5]. For a utility or agency, that is the control point for segmentation between enterprise IT and OT networks, so treat any confirmed compromise as a potential full-network exposure event. 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]. Audit recent policy changes and administrator activity, and get management interfaces off the open internet.
- **Public-facing web estates.** wp2shell exploitation of WordPress continues at internet scale, and compromised sites are being used to attack their visitors with fake Microsoft 365 and banking login overlays; a compromised city or district site would hand attackers your residents as phishing targets [10]. nginx CVE-2026-42533 remains unexploited in public, but a researcher who disputes the vendor's severity assessment says he will publish proof-of-concept details around August 5; close out patch verification before that date [9].

ESPIONAGE: GOVERNMENT WEBMAIL, HOTEL WI-FI, AND THE DNS BLIND SPOT

- **Laundry Bear and Zimbra: local government is a named target.** 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 [6]. Named target sectors include federal and local government, energy, education, law enforcement, and the defense industrial base, which places city halls, district offices, and PSAP administrative networks in scope [6]. Proofpoint additionally reports targeting of what it calls "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 is a common choice where mail budgets are thin, so this is a question to ask across your own estate and your regional partners: patch and upgrade (10.1.20 shipped July 20 with nine additional critical fixes) and hunt for historical compromise [8].

- **Hotel Wi-Fi as a credential trap for traveling operations staff.** ReliaQuest reports an ongoing campaign, active since at least June, in which attackers alter DNS settings on hotel and conference-center Wi-Fi gateways so travelers land on convincing fake Microsoft 365 portals; in some cases the attackers used a device-code sign-in flow that captures a legitimate OAuth session and bypasses MFA outright [11]. Utility engineers at vendor training, conference-bound agency staff, and mutual-aid responders all fit the exposure profile. Public DNS settings do not help, because the compromised gateway forges answers before they reach the resolver [11]. The fix is architectural: full-tunnel VPN before anything else on untrusted networks, encrypted DNS in strict mode, and disabling the Entra device-code flow where the business does not need it [11].
- **DNS as a covert channel.** Fortinet documented a TrickBot-labeled Windows backdoor that runs its command-and-control entirely over DNS queries routed through Google's public resolver, moving 1.2 MB of data in about 40 seconds in testing [12]. The attribution rests on one vendor's code-similarity analysis and the campaign's scale is unquantified, but the defensive lesson stands on its own: an egress policy that inspects HTTP while letting workstations talk DNS to arbitrary external resolvers has a blind spot [12]. Pair this with the hotel-gateway campaign and DNS control earns a place on this quarter's hardening list [11][12].

RANSOMWARE AND EXTORTION: PRODUCTION, CUSTOMERS, AND DESIGN DATA

- **A food and agriculture production halt, and the data now released.** Coca-Cola told regulators on July 16 that a ransomware attack forced it to temporarily suspend US production at fairlife, its dairy subsidiary, after attackers reached production-related systems [14]. The Anubis ransomware group listed fairlife on its leak site July 20, claiming roughly 1 TB of stolen data and setting a publication deadline of Monday, July 27; the volume figure remains an attacker claim [15]. Coca-Cola has since confirmed data was taken and restored a majority of production, and Anubis posted the stolen data for download after the Monday-morning deadline passed [59][60]. For every operator of physical infrastructure, the lesson is the durable one: a production outage does not require OT compromise when production depends on IT systems [14]. Use this case to pressure-test two things in your own house: how quickly you could isolate production-adjacent IT, and who holds the authority to make an extortion-payment decision, on what criteria, with counsel and insurers pre-briefed.
- **Utility customer-data estates are a distinct soft target.** Australia's Origin Energy (about 4.8 million customers) confirmed unauthorized access to customer data including partial payment details, with an extortionist claiming 2 million records; a media report that the threat was privately settled is unverified [16]. Colombia's Ecopetrol disclosed unauthorized access to cloud file storage across roughly 15

subsidiaries in an SEC filing [17]. Billing, CRM, and customer-portal systems are monetizable on their own, and they usually live outside the OT protection program. Extortion aimed at customer data raises the same payment-governance question as the fairlife case, and the unverified "settled" report around Origin shows why that decision framework should exist on paper before an incident [16].

- **Design data lost through a supplier's data center.** In mid-July, the World Leaks extortion group published roughly 19,000 files (14.3 GB) taken from India's Reliance Group via a third-party-hosted server, purportedly including ventilation and cooling blueprints and a control-room floor layout for two under-construction units at the Kudankulam nuclear plant [18]. The plant operator says the material involves only conventional common-service facilities, and the files' authenticity has not been independently verified [18]. The failure mode deserves every infrastructure operator's attention anyway: facility design data left the owner's control through an engineering contractor's outsourced hosting, and the extortionists priced the criticality of the end client rather than the breached party [18]. If EPC firms, engineers of record, or integrators hold your plant drawings, ask where that data physically sits and under what controls.

ELECTION INFRASTRUCTURE: A STANDING WATCH ITEM

This is a standing section through the 2026 cycle, and we will keep it strictly operational. Two developments this week bear directly on election-infrastructure risk.

- **The legal foundation of threat sharing has a hard deadline.** 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 provision and floor opposition exists, so the September 30 sunset remains live [47]. The liability, antitrust, and FOIA protections that underpin ISAC-style sharing lapse if nothing passes [47]. Election offices are among the most dependent consumers of shared threat indicators, and the run-up to a general election is the worst possible moment to discover a sharing channel has gone quiet.
- **Congressional attention is on AI-enabled infrastructure attack.** Members of two House committees ran a first-of-its-kind closed-door exercise simulating AI-enabled cyberattacks against US ports, rail, and airports in a 2027 Taiwan-crisis scenario [53]. The scenario logic applies to any high-visibility civic function, elections included, and the exercise format is a ready template for your own tabletop.

What election offices and their vendors should do now: confirm each election-sector threat-sharing membership you hold is current and that alert routing reaches a monitored inbox; confirm peer-sharing relationships with neighboring jurisdictions and your state election office are current; ask your election-technology and managed-service vendors, in writing, what threat-intelligence channels they consume and how they would notify you of a credible threat; and review with counsel what your indicator-sharing participation looks like if the CISA 2015 protections lapse on September 30 [47]. Schedule a tabletop before the fall that includes an information-blackout scenario, where your usual federal channels are degraded and you must operate on peer and vendor intelligence alone.

TRANSPORTATION, CHARGING INFRASTRUCTURE, AND THE BROADER LANDSCAPE

- **Ports, rail, and airports are the war-game scenario.** The congressional exercise above simulated AI-enabled cyberattacks against exactly the transportation assets this audience runs [53]. Expect transportation and logistics cyber mandates to follow congressional attention, and borrow the scenario for your own exercise calendar before a regulator suggests it [53].
- **Aviation cyber governance, graded.** GAO's new aviation-cybersecurity report (GAO-26-107693) finds the FAA has defined cyber roles while TSA has not, and that TSA's cyber roadmap dates to 2018; both departments agreed with all five recommendations [52]. Worth noting precisely: GAO reports there have been no reports of successful cyberattacks on avionics, so the demonstrated risk concentrates in ground systems and governance, and vendor commentary claiming otherwise is ahead of the evidence [52].
- **EV charging infrastructure is a networked endpoint.** Vendor research published in June showed a production EV fast charger exposing root-credentialed remote access through the charging cable itself, using about $130 in hardware; the finding covers one vendor's model and requires physical access, so resist industry-wide generalization [44]. Utilities and municipalities operating charging networks should still take the frame: chargers are field-deployed, physically accessible network endpoints, and they belong in your asset inventory, patch cycle, and vendor-management program like any other OT device [44].
- **Manufacturing telemetry, as an OT weather report.** SonicWall's new manufacturing brief reports sector intrusion-prevention events down 56.2% year over year yet still totaling 474 million in the first half of 2026, with attacks shifting toward IoT and SCADA entry points; more than half of monitored manufacturing networks saw IoT exploitation attempts, and a single 2021 Hikvision camera flaw drew 43 million hits [54]. The numbers are one vendor's telemetry, skewed toward smaller networks, but the direction matches what we see in the field: perimeter noise is falling while the soft spots move to connected devices, cameras included, and water and power plants run plenty of both [54].
- **AI governance is arriving in procurement.** The Hugging Face incident produced its first legislation: the bipartisan AI Kill Switch Act (H.R. 9917, introduced July 23) would require large AI developers to maintain shutdown capability, report qualifying incidents within 15 days, and comply with graduated federal correction orders during defined loss-of-control scenarios [19][20]. It is one chamber's freshly introduced bill, and passage is far from assured, but boards should expect "could we shut it down, and who orders it?" to become a standard governance question [19]. The incident's practical lesson for anyone deploying AI tools: model-level safeguards are not a security boundary, and effective controls live outside the model, in network rules, scoped credentials, allow lists, and outbound data-loss prevention [22]. Public agencies can also borrow a procurement standard that emerged this week: FedRAMP's director, citing the incident, said vendors who cannot patch critical internet-facing flaws inside FedRAMP 20x's two-to-four-day expectations should exit the federal market; ask your SaaS vendors what their critical-vulnerability clock is, in writing [23].

- **Quick notes.** Any agency running AI browser agents should apply enterprise extension allow-listing: unpatched research shows co-installed extensions can hijack Claude for Chrome's agent actions, and a disputed Claude Code behavior makes repository trust prompts equivalent to code-execution consent [24][25]. A mass sextortion campaign is citing genuinely leaked breach data to look credible, so pre-position plain-language response scripts for residents and employees who receive it [37]. Agencies deploying facial recognition on premises, including AI doorbell-style features, should check biometric-consent posture now given three new proposed class actions in the space [38]. For staff who cross borders with agency devices, the Fourth Circuit's July 13 holding that manual phone searches require no warrant or individualized suspicion strengthens the case for travel devices with minimal local data [39][40].

WHAT YOU SHOULD BE DOING RIGHT NOW

Immediate Actions (This Week)

1. **Act on AA26-097A's July 22 update**: inventory internet-reachable PLCs across Rockwell, Schneider Electric, and Siemens estates, pull them behind secure gateways, run the advisory's new project-file detection guidance, and verify alarm and shutdown logic against engineering baselines [13].
2. **Patch on-premises SharePoint now** (Subscription Edition, 2019, 2016) for CVE-2026-50522, then rotate ASP.NET/IIS machine keys and hunt for webshells and forged-token persistence; assume compromise on servers that sat exposed and unpatched after July 20 [1][2][3].
3. **Patch Check Point Security Management** for CVE-2026-16232, take management interfaces off the internet, restrict access to trusted clients, and audit recent policy changes and admin logins for tampering [1][4][5].
4. **Verify Zimbra patching** (CVE-2025-66376; current release 10.1.20) and hunt for historical webmail compromise going back a year; ask Zimbra-running vendors and neighboring jurisdictions for their status [6][8].
5. **Election offices and vendors: verify threat-intelligence channels**, including current sector information-sharing memberships, alert routing, peer sharing with neighboring jurisdictions, and written vendor answers on threat notification [47].
6. **Pressure-test ransomware decisions**: confirm you can isolate production-adjacent IT quickly, and put the extortion-payment decision framework (authority, criteria, counsel, insurer) on paper before the next fairlife-style deadline [14][15].
7. **Harden 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].
8. **Close the DNS egress blind spot**: restrict workstation DNS to sanctioned resolvers and alert on high-volume or high-entropy DNS to unfamiliar domains [11][12].

9. **Confirm wp2shell and nginx patch completion** on public-facing sites before the announced ~August 5 nginx proof-of-concept; verify auto-updates actually applied [9][10].

Strategic Actions (This Month)

1. **Separate the customer-data protection scope from OT**: inventory billing, CRM, and customer-portal estates, confirm monitoring and MFA coverage, and assign them the same executive attention the grid side gets [16][17].
2. **Review supplier data custody for design and facility documents**: the Kudankulam leak traveled through a contractor's outsourced data center; map where your drawings, control-room layouts, and commissioning records sit in other people's clouds [18].
3. **Schedule a tabletop from the congressional war game**: AI-enabled attack on a port, rail, or airport function, plus an election-season variant with degraded federal threat-sharing channels [53][47].
4. **Track the threat-sharing sunset**: if CISA 2015 lapses September 30, review with counsel what your ISAC and indicator-sharing participation looks like without the liability shield [47].
5. **Put patch-velocity and incident-notification clocks into procurement**: borrow FedRAMP 20x's two-to-four-day standard for critical internet-facing flaws, and add AI incident-notification clauses for any AI-inclusive vendor [23][22].
6. **Bring charging networks and field IoT into the asset program**: treat EV chargers, cameras, and field-deployed devices as networked endpoints with vendor-management requirements to match [44][54].
7. **Add a border-crossing device policy** (travel devices, minimal data, no stored credentials) reflecting the Fourth Circuit's lowered threshold for manual searches [39][40].

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

[59] Coca-Cola Confirms Data Breach After Fairlife Ransomware Attack (SecurityWeek, July 27, 2026) — https://www.securityweek.com/coca-cola-confirms-data-breach-after-fairlife-ransomware-attack/

[60] Coca-Cola Confirms Data Theft in Fairlife Ransomware Attack (BleepingComputer, July 27, 2026) — https://www.bleepingcomputer.com/news/security/coca-cola-confirms-data-theft-in-fairlife-ransomware-attack/

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.

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