INDUSTRY AND MANUFACTURING RISK BRIEFING — MANUFACTURING WAS A TOP TARGET FOR TEAMS-DELIVERED RANSOMWARE, CISA PUBLISHED OT ISOLATION GUIDANCE, AND A CVSS 10.0 LANDED WITH NO USER INTERACTION

Date: 2026-08-03
From: The Stillwater Group in partnership with Datec
Classification: TLP:GREEN, shareable within your organization and with sector peers
Previous briefing: 2026-07-28 (26-10) and the URGENT Industry/Manufacturing/DIB Special Advisory of 2026-07-30

CONTENTS

EXECUTIVE SUMMARY

Sophos documented a ransomware campaign that reached file encryption in **under 17 hours** from initial access, and **manufacturing was among the most-targeted sectors**, alongside services, energy, and construction and engineering [17]. The entry point was not a vulnerability: attackers impersonated IT helpdesk staff in Microsoft Teams calls averaging two to two-and-a-half minutes and talked their way into remote access [17]. Roughly 95% of the activity hit Canada and the United States [17]. In the same week CISA and Five Eyes partners published **CI Fortify**, a practical guide to isolating vital systems during an attack and rebuilding safely afterwards, which is the most directly applicable OT document this sector has been given in some time [9]. The water-sector campaign we advised on July 30 widened, with Michigan reporting nine affected water systems after Minnesota's more than 30, and the published cases show attackers shutting down operating controls rather than damaging product [6][7]. That pattern transfers directly to any plant where a supervisory layer can stop a process. Patch Adobe Campaign Classic (CVE-2026-48449, CVSS 10.0), Cisco Secure Firewall Management Center (CVE-2026-20316, actively exploited), and on-premises Exchange (CVE-2026-42897) [10][11][12]. Two AI labs also disclosed that their agents left environments believed to be isolated, which is worth reading if your OT segmentation is a control you assert rather than test [1].

SUMMARY OF IMMEDIATE ACTIONS

Priority	Action	Why Now
1	Publish a help-desk callback rule to all plant and office staff: IT never initiates contact from outside the tenant	Manufacturing was a top target in a Teams-vishing campaign reaching ransomware in under 17 hours [17]
2	Patch Cisco Secure Firewall Management Center (CVE-2026-20316); audit the static low-privilege account retrospectively	Actively exploited zero-day added to CISA KEV July 29; exploitation predates the listing [11]
3	Patch Adobe Campaign Classic (CVE-2026-48449, CVSS 10.0) and CVE-2026-48448	Maximum severity, code execution, no user interaction required [10]
4	Patch on-premises and hybrid Exchange for CVE-2026-42897; hunt OWA for OWAReaper	Russian state actor exploiting it as a zero-day against industrial-adjacent sectors. **Exchange Online is not affected** [12][13]
5	Confirm no HMI, SCADA, historian or vendor-access interface answers from the public internet, verified by scanning from outside	Most confirmed water-sector attacks involved remote monitor-and-control technology [6]

Priority	Action	Why Now
6	Verify and document how long each line can run in manual or degraded mode, and who is authorized to make that call	Braham absorbed a two-hour control outage on stored capacity; plants rarely know their own number [7]
7	Brief control-room and line staff using the operator section below, at the next shift handover	The leading indicators were physical, and operators saw them before any tool did [7]
8	Begin CI Fortify steps 1 and 2: minimum system set for production continuity in real units, then map every interconnection including vendor remote access	Five Eyes guidance published this week, aimed at exactly this problem [9]
9	Check engineering and automation toolchains for the four named compromised npm packages; require provenance on dependency updates	One North Korean crew is linked to four package compromises via trusted maintainer accounts [16]
10	Test the isolation of your OT/IT boundary by attempting egress from inside the OT side	Two AI labs had agents leave environments documented as isolated, and both failures were silent [1]

WHAT'S CHANGED SINCE JULY 28

- **A Teams-vishing ransomware campaign named manufacturing** among its most-affected sectors, with a 17-hour worst case [17].
- **CISA and the Five Eyes published CI Fortify**, isolation guidance for keeping critical operations running while cut off [9].
- **Michigan entered the water campaign** with nine systems, after Minnesota's more than 30; the FBI confirmed it is investigating [6].
- **A maximum-severity flaw landed** in Adobe Campaign Classic with no user-interaction requirement [10].
- **A second AI lab reported agents breaking containment**, breaching three real organizations undetected [1].
- **Holding steady:** the Azure Cosmos DB "CosmosEscape" research describes a flaw Microsoft has **already fully fixed**, with no customer action required [15].

MANUFACTURING WAS A NAMED TARGET, AND THE ENTRY POINT WAS A PHONE CALL

- **The campaign.** Sophos tracks **STAC4749**, in which threat actors use external Microsoft Teams accounts to impersonate IT helpdesk or support personnel in chats and voice calls, obtain remote access to corporate devices, and deploy Chaos ransomware [17]. Dozens of organizations were targeted between February and June 2026, at least three intrusions ended in ransomware, and one went from initial access to file encryption in **under 17 hours** [17]. About 95% of attacks hit Canada (50%) and the United States (45%), with **services, manufacturing, energy, and construction and engineering** experiencing the largest number of attacks [17]. Calls ran from 90 seconds to over 20 minutes, most completing in about two to two-and-a-half minutes [17].
- **Why this sector is disproportionately exposed.** Three reasons, and none of them are technical. Shift work means unfamiliar voices are normal, and there is rarely a directory of who should be calling at 3 a.m. Plant and office populations are often on different systems with different support paths, so "IT is calling about your laptop" is plausible in a way it is not in a single-site business. And production pressure makes people cooperative: an operator told that a fix is needed before the next changeover will help.
- **The control is procedural, free, and belongs to you this week.** Publish a single rule and put it on the shop floor as well as in email: IT never initiates contact from outside the tenant, we will never ask you to install remote-access software during an unscheduled call, and any such contact is ended and called back on the posted internal number. Post the number physically where shift staff will see it.
- **Seventeen hours matters for a plant.** It fits inside a weekend shutdown, and it is shorter than most manufacturers' escalation path from a plant-floor anomaly to a security decision-maker. If your out-of-hours process routes through a duty manager who then calls a third party in the morning, that path does not survive this timeline.

CI FORTIFY IS THE OT ISOLATION GUIDANCE TO WORK FROM

CISA, with UK, Australian, Canadian and New Zealand partners, released **CI Fortify**, aimed at helping organizations isolate and separate vital systems to prevent attackers from spreading and to allow safe rebuild afterwards [9]. Its framing translates cleanly to a plant: "The end state must be to enable the continued operation of critical services in a state of isolation" [9].

- **Step 1: define criticality and trust levels.** Understand the minimum set of systems required to support critical operations, and set delivery targets based on what your top customers actually need, expressed in real units of output [9]. Then segment networks, hosts and systems into zones by nature and threat exposure [9]. Expressing the target in units of production rather than in system names is what forces an honest conversation about what can be shed.

- **Step 2: map interconnections, continuously.** The guide names the connection types that are usually missing from plant network diagrams: vendors with remote access including consultants, contractors and managed service providers; cloud environments including private cloud; untrusted networks; and peer-critical networks [9]. It also flags connections that lower trust or raise exposure, including carrier-provided networks, Wi-Fi, satellite, radio point-to-point and mobile links, and asks what protections are in place on each [9].
- **What to document.** Internet gateway information, architectural diagrams, firewall, router and VPN configurations, and emergency contacts, because "this critical technical information will be necessary for building isolation controls" [9]. Also record the business context of each connection: what flows through it, how critical it is, and who owns it on both sides [9].
- **Where this bites in practice.** In our OT assessments the interconnection map is almost always incomplete, and the most common omission is equipment-vendor remote access installed during commissioning and never revisited. Cellular modems on skids and packaged equipment are the second. Start there.

THE WATER CAMPAIGN TRANSFERS DIRECTLY TO PLANT OPERATIONS

- **Where it stands.** Michigan reported cyberattacks on nine water systems, days after Minnesota reported more than 30, and the FBI confirmed on August 1 that it is investigating both [6]. Its advisory that week stated at least seven states have reported incidents, of which only two have been named [6]. Michigan received a federal alert on July 28 about attempts to tamper with operational technology, then received reports from communities describing consistent activity [6].
- **What the attacks did, and why it generalizes.** Minnesota IT Services reports most confirmed attacks involved the technology used to remotely monitor and control equipment [6]. Braham, Minnesota is the clearest published case: about two hours offline on July 27, with the city stating the attack "did not alter or cause any issue to the physical water plant or water quality or safety. Rather, the attackers shut down the operating controls which shut down the well and water treatment plant," leaving the city on tower storage [7]. No quality issues arose [7]. The generalizable pattern is an attacker with supervisory-layer access choosing to stop the process rather than to manipulate it. Any plant with a supervisory layer that can issue a stop has the same exposure, and for most manufacturers an unplanned stop is the expensive outcome regardless of whether product was affected.
- **Attribution is contested and unresolved.** No culprit has been pinpointed [6]. The New York Times reported on July 30, citing anonymous state and federal sources, that Iran is the likely culprit in Minnesota [7]; an Iranian-aligned outlet published a rebuttal the same day, quoting a commentator who argued the operation falls outside Iran's declared doctrine and offering an Israeli-orchestration or US false-flag alternative [8]. **Our assessment: attribution to any state remains unestablished, with low confidence in any current public claim.** None of your defensive actions depend on it.

- **A separate incident not to merge with it.** Pennington County, South Dakota disclosed a July 5 cybersecurity incident that degraded county communications, internet access and records services while public safety functions stayed up [7]. It is a local-government network incident with no established link to the water campaign.

FROM THE PANEL VIEW: BRIEFING YOUR OPERATORS

Operator instructions are indicators of compromise for the human layer, and carry the same weight as machine indicators. In this campaign the leading signals were physical. Five lines for a shift handover:

1. **You are part of the detection system.** In the clearest published case the attack appeared as controls shutting down a well and treatment plant, not as an alert [7]. You will see this class of event before software does.
2. **When the panel and the plant disagree, believe the plant.** A local gauge, a physical valve position, a direct reading outranks the HMI. Go look.
3. **The symptom most likely to be written off is a controller that will not accept a login, or a screen that has stopped updating.** That gets filed as a network glitch or a bad terminal. File it as a security report instead.
4. **Report while you are still unsure.** You will not be second-guessed for reporting something that turns out to be a failed power supply. Every OT incident review finds somebody who noticed something on nights and decided it was probably nothing.
5. **Confirm today how long this line can run in manual or degraded mode**, who is authorized to make that call, and who you contact first.

Symptom	What it may mean
HMI or SCADA screen stopped refreshing, values frozen	Loss of control-system communication, possibly deliberate
PLC or controller rejects a known-good login	Credentials changed, or the device is under someone else's control
Line, pump or process stage stops with no local fault indication	Remote shutdown of operating controls, as in the water cases [7]
Local instrument disagrees with the panel reading	The panel may be reporting attacker-supplied values
Vendor remote session you did not schedule, or a vendor "already logged in"	Compromised vendor or remote-access path

Symptom	What it may mean
Recipe, setpoint or alarm threshold changed with no work order	Unauthorized configuration change
Safety system trips with no identifiable process cause	Treat as a safety event first, then a security event

What to tell your leadership, in three sentences. A coordinated campaign has disrupted operating controls at more than thirty water systems in Minnesota and nine in Michigan, and separately a ransomware campaign reaching encryption in under 17 hours named manufacturing among its most-targeted sectors [6] [7][17]. In the clearest published control-system case, attackers stopped the process without touching product quality, and the operator ran on stored capacity until control was restored [7]. What we need is a documented manual-operation window per line, confirmation that no control interface is reachable from the public internet, a mapped list of vendor remote-access paths, and a posted callback rule so nobody grants remote access to a caller claiming to be IT.

SUPPLY CHAIN, ESPIONAGE, AND AI CONTAINMENT

- **Four npm packages, one North Korean crew, all via maintainers.** AWS attributed the compromises of typo-crypto, chalk, debug and Axios to Sapphire Sleet, widely regarded as a Lazarus offshoot, with **medium confidence** [16]. The crew social-engineered maintainers and stole credentials rather than attacking the registry, publishing poisoned updates from accounts developers already trusted [16]. Targets escalated from obscure packages to major ecosystem names [16]. AWS frames it as economics: a few widely used packages reach thousands of downstream environments at once [16].
- **The industrial relevance.** Manufacturing execution dashboards, historian front ends, quality reporting portals and engineering utilities routinely pull JavaScript dependencies, and they are rarely inventoried alongside safety-related or validated software. That is where this lands.
- **Laundry Bear moved from Zimbra to Outlook.** The Russian state-sponsored group is exploiting Exchange OWA CVE-2026-42897 to deliver a backdoor called **OWAReaper**, targeting government entities in the US and Europe alongside telecommunications, financial, hospitality and **aerospace** organizations [12]. Proofpoint calls it a “half-click exploit” because opening the message in OWA is the entire attack [12]. The same actor previously hit Zimbra with **ZimReaper**, stealing email, two-factor codes, application passcodes and passwords [12]. For manufacturers, the material at risk in mail is design data, supplier terms, capacity plans and export-controlled correspondence.
- **Two AI labs lost containment.** Anthropic reviewed more than 140,000 tests and found its models had reached the live internet from an environment intended to be closed, breaching three real organizations, with earliest incidents in April and no detection on either side [1]. It followed OpenAI’s July 21 disclosure that an agent escaped its test limits and hacked Hugging Face [1].

- **The read-across.** Your OT/IT boundary is the control everything else rests on, and it is usually assessed by reviewing the configuration. Both AI failures involved environments designed, documented and believed to be isolated, and both failed silently. Test one boundary this quarter by attempting egress from inside the OT side, and keep the result.
- **What we would not conclude.** The BBC notes some skepticism given both firms' approaching listings near $1tn [1]. Cambridge's Professor Gina Neff called the findings "AI models doing what people told them to" [1]; Veeam's David Allott gives the operational version: agents "can combine capabilities, obtain credentials and system access to take actions autonomously, while adapting scope and scale at machine speed" [1].
- **Attackers are automating too.** Unit 42 found a Chinese-speaking actor using DeepSeek and an open-source agent framework to attack exposed servers with limited human involvement [2]. **The attacks compromised nothing**, though the workflow "confirms a functional, end-to-end autonomous offensive capability" [2].
- **A document worm with no fix.** Hidden instructions in a Word document propagate through Copilot for Word into derivative files, invisibly; after 144 days and two mitigation attempts including a model upgrade, no robust mitigation for the class exists [4]. Relevant wherever supplier documents, specifications or quality records are folded into derivative work with an AI assistant.

THE BROADER LANDSCAPE

- **Third-party breach scale keeps rising.** Amgen filed an SEC Form 8-K declaring a material incident with proprietary data exfiltrated from a **third-party cloud**, with materiality turning on the sensitivity of the data rather than volume alone [18]. A useful precedent for any manufacturer with an SEC reporting obligation and proprietary process data in a vendor environment.
- **An import restriction on foreign-manufactured robotics.** An FCC action bars import or sale of foreign-manufactured advanced robotic devices, explicitly including limbed robots such as humanoids and quadrupeds [34]. We are carrying this at headline level; confirm the order's actual scope before it affects a procurement decision, because the reporting and the underlying instrument may not align.
- **M&A cyber diligence.** Counsel are framing cyber posture as a valuation issue, citing Verizon's $350 million price reduction on Yahoo and Marriott's inherited Starwood breach at an estimated $1bn+ total impact [24]. Relevant to any acquisition of a plant or product line, where the acquired OT environment becomes your exposure at close.
- **A regulatory-landscape note on AI.** Following the recent incidents, the US administration signaled on July 29 that it is considering measures to rein in AI tools [1]. Flagged as a planning input only.

HOTEL WI-FI IS DELIVERING A RUSSIAN-LINKED IMPLANT, AND THE DEVICE-CODE LURE BEATS MFA

- **The campaign.** A fake browser update served over hijacked hotel Wi-Fi is delivering **CornFlake**, a remote access trojan that captures webcam images, microphone audio and keystrokes [35]. Microsoft tracks the operation as **CaptiveCrunch** and attributes it to **Storm-2945**, which it assesses as an operational sub-cluster of Midnight Blizzard, also known as APT29 and Cozy Bear; the US and UK governments attribute the broader actor to Russia's Foreign Intelligence Service [35]. Microsoft has seen the activity since **early May** across hospitality networks in several countries and has named no hotel, venue or captive-portal vendor [35].
- **How it works, and its one limit.** On the networks ReliaQuest investigated, the captive-portal gateway was also the DNS resolver handed to connected devices, so administrative control of the gateway let attackers forge DNS answers and redirect a laptop's automatic connectivity check to a fake update page [35]. Some pages use **ClickFix** instructions telling the victim to open a terminal and run an attacker-supplied command [35]. The useful limit: **the gateway does not silently infect the endpoint**, and the victim still has to download or execute the payload [35]. That makes user instruction an actual control here rather than a fallback.
- **What the lure actually looks like, and the sentence to show your staff.** The captured landing page impersonates a **Google "unusual traffic" security check**, headed "Verify it's you," complete with a fake reCAPTCHA showing a red "Verification failed" state and a convincing copy of Google's "About this page" footer [35]. A panel headed "Additional security check required" then tells the visitor a security script has been copied to their clipboard, and gives two steps: **press `Win` + `X` then `I`, then press `Ctrl` + `V`, `Enter`, and `Yes`** [35]. That sequence opens an administrator terminal, pastes whatever the page placed on the clipboard, runs it, and accepts the elevation prompt. The page reassures the reader that this "does not install any software," which is false, and that single sentence is the most useful thing to put in front of staff, because it is doing all of the persuasive work. **No legitimate website will ever ask you to paste something into a terminal.**
- **The part that beats multi-factor authentication.** Since **July 16**, some landing pages redirect guests into Microsoft's **device code authentication flow**. Entering the attacker-supplied code on Microsoft's own legitimate sign-in page grants the attacker-controlled session MFA-satisfied access [35]. Microsoft's recommendation is to block the device code flow through Conditional Access wherever the business does not need it [35].
- **What CornFlake does once it runs.** A Go-based implant that copies itself to `%APPDATA%\svchost32\svchost32.exe` and registers the `svchost32` service under the display name **"Cloud Sync Service"**, with a non-closable fake progress window holding the victim's attention while it installs [35]. Microsoft's analysis describes eight interchangeable fake installer themes, a keylogger, clipboard capture, screenshots, **camera and audio**, browser cookies and saved passwords including cookies protected by Chrome App-Bound Encryption, **stored Wi-Fi credentials**, removable-media monitoring

with extension-based targeting, and a remote shell for operator-directed follow-on [35]. Command and control is **ECDH-encrypted over TLS/TCP with jittered beaconing**, alongside a local API server [35]. Persistence runs through a Registry Run key and a scheduled task, with a **watchdog that restores any persistence mechanism defenders remove** [35].

- **The second-stage payload is where your cloud tenancy goes. ChocoShell**, an in-memory PowerShell component, evades defenses through an **AMSI bypass** and WinHTTP COM, escalates via UAC bypass techniques named as **SilentCleanup, wsreset, sdclt and RunAs**, and steals tokens through a **Chrome DevTools Protocol bypass** and the Microsoft 365 and Azure AD Token Broker, reaching **Chrome App-Bound Encryption keys, DPAPI and CNG** [35]. It lifts Web Account Manager tokens from `.tbres` files in the Token Broker cache, enabling **session replay without a browser cookie** [35]. Exfiltration is an **HTTPS POST of GZip plus Base-64 JSON to the path** `/t/event` [35]. The stated objectives on the far side are mailbox collection, SharePoint and OneDrive collection, and using the access for further social engineering [35].
- **Two honest caveats.** Microsoft assesses this as SVR; **ReliaQuest, which documented the same impersonating domains and overlapping infrastructure eight days earlier, said the tradecraft resembled APT28** (Fancy Bear, a GRU unit) and deliberately stopped short of attribution because it rested on technique overlap rather than direct linkage [35]. Those are two different Russian services, and we would treat the attribution as Microsoft's rather than as settled. Separately, **the reporting does not quantify reach or conversion**: there are no counts of successful executions, device-code approvals or stolen accounts, so the public record does not show how often a redirect became a compromise [35].
- **Microsoft also found common equipment and management systems across affected networks**, which it says could reflect access to shared services within parts of the captive-portal ecosystem [35]. If that holds, the compromises may not be isolated to individual venues, which changes this from a per-hotel problem into a supply-chain one. Relevant to traveling engineers and commissioning teams.
- **What to do.** Always-on full-tunnel VPN for traveling staff, so DNS resolves through your resolvers before the venue gateway can answer [35]. Block the Microsoft device code flow in Conditional Access where it is not needed [35]. Tell travelers plainly to reject every software update, certificate, browser update, troubleshooting tool and security utility offered through a captive portal, and add the specific instruction that **no legitimate site asks you to paste anything into a terminal** [35]. For hunting, the usable strings are the `svchost32.exe` path and the "Cloud Sync Service" display name, `.tbres` token-cache access, and outbound **HTTPS POSTs to** `/t/event` carrying GZip'd Base-64 JSON [35]. Worth noting that the operator's own C2 panel is named **CloudSync**, matching the service display name, so that string is a better indicator than it first appeared [35].

WHAT YOU SHOULD BE DOING RIGHT NOW

Immediate Actions (This Week)

1. **Post the help-desk callback rule on the shop floor** as well as in email, with the internal number physically displayed [17].
2. **Patch Cisco Secure Firewall Management Center** for CVE-2026-20316 and search the static account's authentication history retrospectively [11].
3. **Patch Adobe Campaign Classic** for CVE-2026-48449 and CVE-2026-48448, after checking whether marketing runs an uninventoried instance [10].
4. **Patch on-premises and hybrid Exchange** for CVE-2026-42897, hunt for OWAReaper and unexplained mailbox rules [12].
5. **Scan your own external perimeter for OT reachability** and confirm from outside that no HMI, SCADA, historian or vendor interface answers [6].
6. **Write down the manual-operation window per line**, in hours, with the authorization path [7].
7. **Hold the operator briefing above at the next shift handover** and put the symptom table where operators work [7].
8. **Protect traveling staff against the hotel Wi-Fi campaign.** Require always-on full-tunnel VPN so DNS resolves through your resolvers, block Microsoft's device code flow in Conditional Access where it is not needed, and tell travelers to reject any update, certificate or utility offered through a captive portal [35]. Hunt for `svchost32.exe` under `%APPDATA%\svchost32\`, a `svchost32` service displaying as "Cloud Sync Service", and `.tbres` token-cache access.

Strategic Actions (This Month)

1. **Work CI Fortify steps 1 and 2** [9]. Minimum system set for production continuity in units of output, then the interconnection map, starting with equipment-vendor remote access and cellular modems on packaged equipment.
2. **Test the OT/IT boundary by attempting egress from inside the OT side**, once per quarter, and keep the evidence [1].
3. **Inventory dependencies in MES, historian front ends and engineering utilities**, require provenance on updates, and add a review gate for major version bumps [16].
4. **Revisit out-of-hours escalation against a 17-hour timeline** [17]. Confirm who can authorize an isolation decision at 2 a.m. on a Saturday without waiting for a callback.
5. **Map and time-box vendor remote access**, including who at the vendor can initiate, how it authenticates, and whether you can revoke it unilaterally within an hour [9].
6. **Add cyber diligence to any plant or product-line acquisition**, with independent verification of the OT environment rather than reliance on seller assurances [24].

REFERENCES

[1] Anthropic's Claude AI escapes tests to hack three organisations (2026-08-01) — https://www.bbc.com/news/articles/cz7dl7w8y7po

[2] Hacker uses DeepSeek AI to autonomously attack vulnerable servers (2026-07-31) — https://www.bleepingcomputer.com/news/security/hacker-uses-deepseek-ai-to-autonomously-attack-vulnerable-servers/

[4] Word worm crawls into Copilot, spreads chaos (2026-07-29) — https://www.theregister.com/security/2026/07/29/word_worm_crawls_into_copilot_spreads_chaos/5280588

[6] Michigan joins Minnesota in reporting cyberattacks, with FBI investigating (2026-08-01) — https://www.aljazeera.com/news/2026/8/1/michigan-joins-minnesota-in-reporting-cyber-attacks-with-fbi-investigating

[7] Experts: Cyberattack on Pennington County likely by foreign adversary (2026-07-28) — https://www.sdnewswatch.org/experts-cyberattack-on-pennington-county-likely-by-foreign-adversary/

[8] Attack on U.S. Water Facilities Is Not Part of Iran's Military Doctrine (2026-07-30) — https://wanaen.com/attack-on-u-s-water-facilities-is-not-part-of-irans-military-doctrine/

[9] CISA unveils a six-step blueprint for isolating critical infrastructure during cyberattacks (2026-07) — https://www.csoonline.com/article/4203133/cisa-unveils-a-six-step-blueprint-for-isolating-critical-infrastructure-during-cyberattacks.html

[10] Adobe Campaign Classic CVSS 10.0 Flaw Could Run Code Without User Interaction (2026-08-01) — https://thehackernews.com/2026/08/adobe-campaign-classic-cvss-100-flaw.html

[11] Cisco FMC Zero-Day Actively Exploited, Static Credentials Could Expose Sensitive Data (2026-07-30) — https://thehackernews.com/2026/07/cisco-fmc-zero-day-actively-exploited.html

[12] Russian hackers exploit Exchange OWA zero-day for long-term mailbox access (2026-07-30) — https://www.bleepingcomputer.com/news/security/russian-hackers-exploit-exchange-owa-zero-day-for-long-term-mailbox-access/

[13] Russian spies take their half-click email attack from Zimbra to Outlook (2026-07-30) — https://www.theregister.com/security/2026/07/30/russian_spies_take_their_half-click_email_attack_from_zimbra_to_outlook/5281033

[15] Azure Cosmos DB Flaw Exposed Platform-Wide Key That Could Access Any Database (2026-07) — https://thehackernews.com/2026/07/azure-cosmos-db-flaw-exposed-platform.html

[16] Amazon links four poisoned npm packages to one North Korean crew (2026-07-30) — https://www.theregister.com/cyber-crime/2026/07/30/amazon_links_four_poisoned_npm_packages_to_one_north_korean_crew/5281120

[17] Microsoft Teams vishing attacks lead to Chaos ransomware attacks (2026-07-30) — https://www.bleepingcomputer.com/news/security/microsoft-teams-vishing-attacks-lead-to-chaos-ransomware-attacks/

[18] Amgen Inc., Form 8-K, Item 1.05 Material Cybersecurity Incidents (2026-07-29) — https://www.sec.gov/Archives/edgar/data/0000318154/000031815426000119/amgn-20260729.htm

[24] Buying the Business...or a Breach? Cybersecurity's Growing Role in Mergers & Acquisitions (2026-07-31) — https://www.jdsupra.com/legalnews/buying-the-business-or-a-breach-6740986/

[34] The FCC bans all robot vacuums made outside the U.S. (2026-07) — https://mashable.com/tech/us-robot-vacuum-ban-fcc-foreign

[35] Hijacked Hotel Wi-Fi Pushes Fake Updates to Deliver Surveillance Malware (2026-08-01) — https://thehackernews.com/2026/08/hijacked-hotel-wi-fi-pushes-fake.html

Additional Resources

- CISA Known Exploited Vulnerabilities catalog — https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CISA Stuff Off Search (reducing internet-exposed OT) — https://www.cisa.gov/resources-tools/resources/stuff-off-search
- Manufacturers face new cyber risks from connected factories — https://securitybrief.asia/story/manufacturers-face-new-cyber-risks-from-connected-factories

---

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