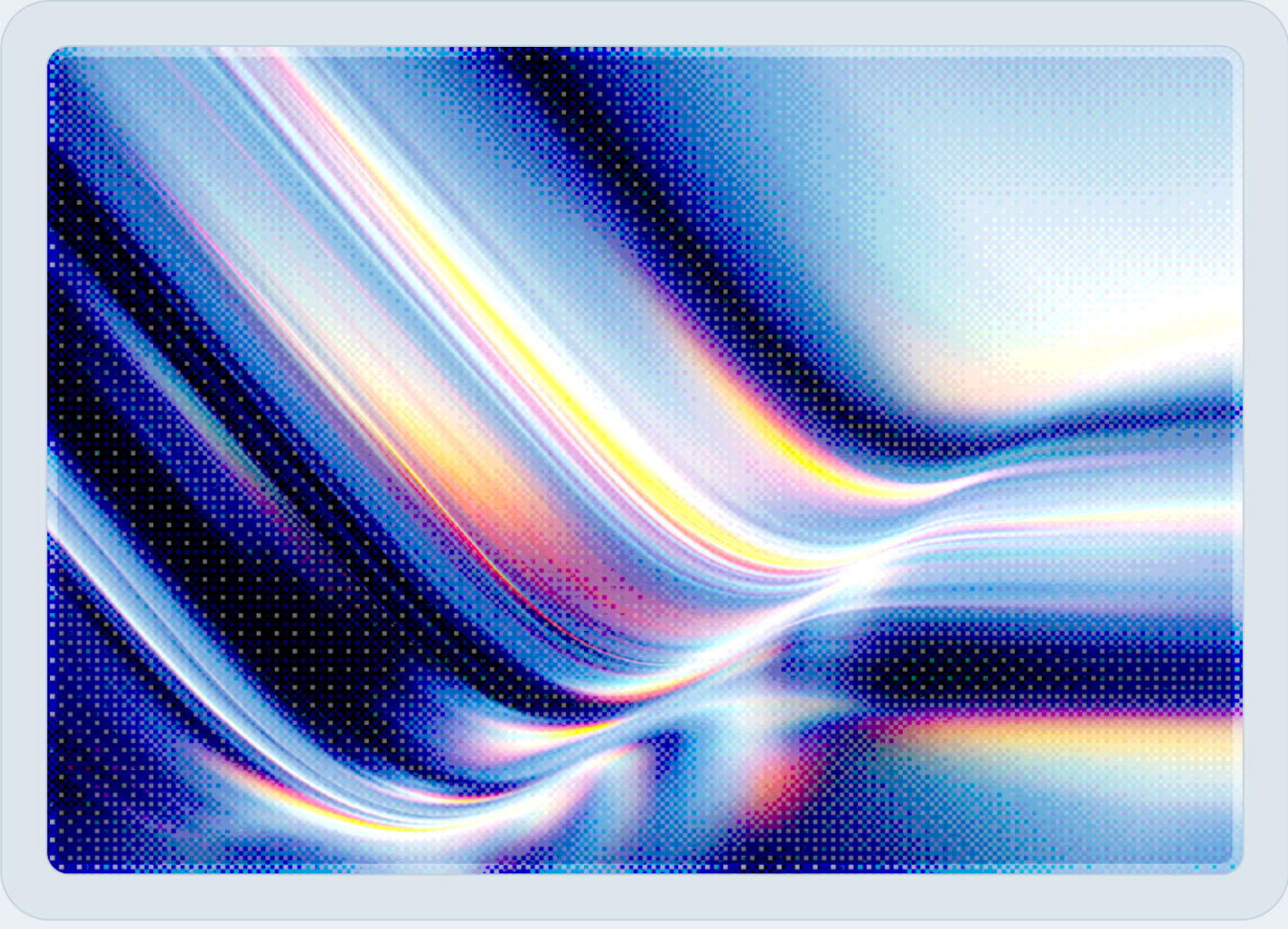
CSAI Foundation | Cloud Security Alliance

Coordinated OT Attack Disrupts 30+ Minnesota Water Utilities

Suspected Iran-Linked PLC Exploitation Exposes Small-Utility Gaps

2026-07-31

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Key Takeaways

- Over the weekend of July 26–27, 2026, a coordinated cyberattack struck operational technology at more than 30 municipal water and wastewater utilities across Minnesota, with Braham, Plymouth, South St. Paul, and Maple Plain publicly confirming impact to automated control functions tied to water towers and lift stations [1][2].
- In Braham, attackers locked out operating controls entirely, forcing the treatment plant offline for two to three hours, depending on the source, before staff restored operations through manual overrides; the city also asked residents to minimize water use during the outage, and other affected utilities disconnected cellular modems linking remote OT equipment to contain the intrusion [1][4][6][7].
- Minnesota IT Services (MNIT) confirmed the incident on July 28, activated its incident response capabilities, and is coordinating containment, recovery, and threat-intelligence sharing with CISA, the EPA, the FBI, and the affected utilities; no impact to drinking water quality has been reported [2][5].
- The intrusions followed by four days a July 22 update to CISA Advisory AA26-097A, which expanded documented Iranian-affiliated PLC exploitation beyond Rockwell Automation controllers to include Schneider Electric Modicon M340 and Siemens S7-1200 devices, and added detection guidance for tampering with reusable code modules inside PLC programs [3].
- Security researchers at Tenable have tentatively attributed the pattern to the IRGC-linked group CyberAv3ngers based on the timing relative to the advisory update and the coordinated, multi-site targeting profile, though U.S. officials have not issued a formal attribution and are still investigating [3][11][12].
- A central technical driver is CVE-2021-22681, a CVSS 9.8 authentication-bypass flaw in Rockwell Automation Logix controllers and the Studio 5000 Logix Designer engineering software that has no available vendor patch and was added to CISA's Known Exploited Vulnerabilities catalog in March 2026 based on confirmed exploitation; CISA and Tenable have since linked broader PLC-targeting activity under this and related CVEs to Iranian-affiliated actors as part of the AA26-097A advisory campaign [3][10][13].

Background

Minnesota IT Services disclosed on July 28, 2026 that operational technology at more than 30 community water and wastewater systems across the state had been targeted in a coordinated cyberattack over the preceding weekend [2][5]. The affected utilities span small and mid-sized municipalities rather than a single large system, and four cities — Braham, Plymouth, South St. Paul, and Maple Plain — have publicly described impacts to automated control functions governing water towers, lift stations, and treatment processes [1][6]. Braham's experience illustrates the severity attackers achieved at individual sites: intruders locked local operators out of their own control system, forcing the treatment plant into an outage that press accounts put at roughly two to three hours before staff restored service through manual overrides rather than the automated controls the attackers had seized [1][7]. Other utilities responded by proactively disconnecting the cellular modems that link remote OT equipment, such as pumps and level sensors, back to central control systems, trading remote visibility for containment. MNIT's initial July 28 statement said the agency was not aware of any utility asking residents to change their water use, but Braham subsequently asked residents to minimize water use during its outage; MNIT has reported no confirmed impact to drinking water quality, indicating that the manual-fallback procedures water utilities routinely maintain for safety reasons functioned as intended even when digital controls were compromised [2][4][6].

The incident's timing places it squarely within a broader pattern of PLC exploitation that CISA, the FBI, and the EPA had already been tracking. On July 22, 2026 — four days before the Minnesota intrusions began — CISA updated Advisory AA26-097A to expand the scope of observed Iranian-affiliated PLC exploitation beyond the Rockwell Automation CompactLogix and Micro850 controllers named in earlier versions to include Schneider Electric Modicon M340 and Siemens S7-1200 devices, and it documented, for the first time, exfiltration of controller project files alongside new detection guidance for manipulation of reusable code modules embedded in PLC programs [3]. That update reflected a technique CISA had already linked to Iranian-affiliated actors: rather than exploiting a single software flaw, attackers connect to internet-facing PLCs from foreign hosting infrastructure using the same engineering software — Rockwell's Studio 5000 Logix Designer — that legitimate plant operators use for configuration, then download and modify controller project files and alter the data shown on operator displays [3]. Because that access method authenticates as a legitimate engineering session rather than triggering a conventional exploit signature, CISA's advisory suggests it is difficult for utilities running standard IT-focused monitoring to distinguish from routine maintenance traffic [3].

Attribution for the Minnesota intrusions remains provisional. Tenable's security researchers have pointed to the IRGC-linked group publicly tracked as CyberAv3ngers, citing the four-day gap between the AA26-097A update and the start of the attacks, as well as a multi-site coordination pattern uncommon in unrelated municipal IT failures [3][11]. CyberAv3ngers has a documented history of targeting U.S.

water utilities: beginning in late 2023, the group compromised at least 75 internet-exposed Unitronics PLCs at water utilities in the United States and abroad, relying in that earlier campaign on factory-default credentials rather than the Studio 5000 authentication-bypass technique associated with the current advisory [16]. U.S. federal agencies, including CISA, the FBI, and the EPA, are working with MNIT to determine the initial access vector, the full scope of affected systems, and whether the Minnesota intrusions are connected to a wider campaign against water-sector OT nationally, and officials have not issued a formal attribution as of this writing [1][8].

Security Analysis

An Authentication Gap With No Vendor Fix Appears to Be the Central Technical Driver

The technical center of gravity for this campaign is CVE-2021-22681, an insufficiently protected cryptographic key in Rockwell Automation's Logix Designer authentication mechanism that allows a remote, unauthenticated attacker to bypass verification and connect to a targeted controller by mimicking a trusted engineering workstation [10][13]. First disclosed in February 2021, the flaw affects a wide range of Logix-family controllers, including CompactLogix, ControlLogix, DriveLogix, FlexLogix, GuardLogix, and SoftLogix devices, and it carries a CVSS score of 9.8 [13]. CISA added it to the Known Exploited Vulnerabilities catalog in March 2026, five years after initial disclosure, based on confirmed exploitation; CISA and Tenable have since tied broader PLC-targeting activity under this and related CVEs to Iranian-affiliated actors through the AA26-097A advisory — a gap that underscores how long a vulnerability without a comprehensive vendor patch can remain a live threat once the mitigating assumption, that the flaw is theoretical rather than weaponized, no longer holds [3][10][13]. The advisory's July 22 expansion to Schneider Electric and Siemens devices suggests the underlying weakness is not confined to one vendor's authentication design; rather, it reflects a broader class of engineering-protocol trust models across PLC vendors that assume any client presenting valid vendor engineering software is a legitimate operator, an assumption this campaign shows can no longer be relied upon [3].

Legitimate Engineering Tools as the Attack Path Appear to Defeat Signature-Based Defenses

What distinguishes this campaign from earlier water-sector intrusions, such as CyberAv3ngers' 2023 Unitronics campaign built on default credentials, is that attackers are using the vendor's own engineering software to reach controllers rather than a conspicuously anomalous tool [3][16]. Downloading and modifying controller project files through Studio 5000 Logix Designer, and altering the values shown on operator displays, are actions a legitimate technician performs routinely; an attacker performing the same actions from foreign-hosted infrastructure looks identical at the protocol level unless a defender is specifically monitoring for the origin and context of that session, not just its content [3]. This is precisely the scenario CISA's detection guidance for reusable code module manipulation was written to address, and it is consistent with why utilities recovering from this incident have leaned on manual operational overrides rather than the automated controls attackers demonstrated they could manipulate [3][7].

Small-Utility Operating Realities Appear to Have Shaped Both the Damage and the Response

The multi-site, coordinated nature of the Minnesota campaign — more than 30 utilities affected roughly simultaneously — is consistent with opportunistic scanning for internet-exposed PLCs across a state rather than the targeting of any single high-value facility. That pattern is consistent with what federal auditors have described as a structural exposure across the water sector: the Government Accountability Office has repeatedly found that the EPA lacks a comprehensive, risk-based strategy for water-sector cybersecurity, and that many small and rural systems face workforce shortages and aging technology that is difficult to secure even as they rely on remote connectivity, including cellular modems, for basic operational visibility [1][7][17]. That same structural reality shaped the response: the affected communities' ability to isolate cellular modems and revert to manual control, together with MNIT's ability to dispatch incident-response support to small-town operators who lack in-house capacity for network cleanup and forensic triage, appear to have been central to preventing the incident from escalating into a water-quality or supply event [7][8]. The absence of any reported water-quality impact should not be read as evidence the underlying exposure is minor; it reflects the success of physical and procedural safety fallbacks that exist independently of the digital controls attackers actually compromised.

Recommendations

Immediate Actions

Water and wastewater utilities, particularly small and mid-sized systems with internet-facing Rockwell, Schneider Electric, or Siemens PLCs, should treat CISA Advisory AA26-097A as an active operational alert rather than background reading, and should inventory every PLC reachable from the public internet or through cellular modem gateways to determine whether it falls within the advisory's expanded scope [3]. Utilities using Rockwell Logix-family controllers should apply Rockwell's published mitigations for CVE-2021-22681, since no comprehensive vendor patch exists, and should independently verify whether engineering-software access to their controllers is restricted to an isolated network segment rather than reachable from the general internet [10][13]. Any utility that identifies anomalous engineering-session activity, unexpected changes to controller project files, or discrepancies between operator-display data and physical process readings should isolate the affected PLC, revert to manual control, and report the activity to CISA, the EPA, and MNIT or the relevant state IT authority immediately, following the same containment pattern the affected Minnesota utilities used [2][7].

Short-Term Mitigations

Utilities should disable or tightly restrict remote cellular modem access to OT equipment except during scheduled maintenance windows, since these gateways were a primary vector affected communities had to sever during containment, and should replace any remaining factory-default or shared credentials on internet-reachable devices, closing the exposure class CyberAv3ngers previously exploited in its 2023 Unitronics campaign [7][16]. In parallel, CISA's July 30 guidance for the water sector recommends removing publicly exposed PLCs from the internet entirely, routing any necessary remote access through a VPN or gateway device, enabling password protection in place of default credentials, and allowlisting the specific IP addresses of known engineering laptops rather than permitting open remote access [9]. Because the current campaign works by mimicking legitimate engineering sessions rather than exploiting an obviously anomalous tool, utilities should implement logging and alerting specifically for Studio 5000 Logix Designer and equivalent engineering-software connections that originate from outside the expected internal network range, rather than relying solely on IT-focused intrusion detection tuned for conventional malware [3]. Small utilities lacking dedicated OT security staff should engage the no-cost assessment and incident-response resources CISA and the EPA make available to the water sector, following the coordination model MNIT used to extend state-level incident response to affected small-town operators during this event [8].

Strategic Considerations

The water sector's exposure in this incident reflects a structural mismatch between decades-old PLC authentication models, which assume any client running vendor engineering software is trustworthy, and a threat environment in which state-linked actors now actively scan for and exploit exactly that assumption across multiple vendors simultaneously [3][10]. Utilities and their state IT partners should prioritize network segmentation that separates OT engineering access from any internet-reachable path, following a zone-and-conduit model rather than relying on point patches for individual CVEs, since this campaign's expansion across three PLC vendors within a single advisory update shows the underlying trust-model weakness generalizes beyond any one manufacturer's fix cycle. Given the sector's reliance on thousands of small, resource-constrained operators, state and federal programs should continue expanding shared incident-response capacity of the kind MNIT deployed here, since individual small utilities cannot reasonably be expected to independently detect nation-state-grade PLC exploitation techniques that authenticate as legitimate maintenance activity.

CSA Resource Alignment

CSA's "Zero Trust Guidance for Critical Infrastructure" is the most directly applicable prior CSA artifact for this incident, since it was written specifically to apply Zero Trust principles to the OT and ICS environments this campaign targeted, using the same zone-and-conduit and Purdue Model concepts that underlie the network-segmentation recommendation above [14]. That guidance documents the structural conditions this incident exemplifies — in broad terms, its research describes a majority of surveyed OT systems running outdated operating systems, a substantial share with direct internet connections or remotely accessible devices, and OT environments that get patched far less frequently than conventional IT systems — conditions that map directly onto a five-year-old, still-unpatched Rockwell authentication flaw being actively exploited across multiple state water utilities [14]. Its five-step implementation process, beginning with defining a protect surface around critical control functions and mapping operational flows before building enforcement policy, offers affected utilities and their state partners a concrete methodology for closing the internet-facing PLC exposure this campaign relied on, rather than treating the incident as resolved once the immediate intrusion is contained.

CSA's AI Controls Matrix (AICM) v1.1 provides the broader control vocabulary relevant to two aspects of this incident even though the campaign itself did not involve AI systems: its threat and vulnerability management domain addresses the kind of long-lived, unpatched vulnerability management gap CVE-2021-22681 represents, and its identity and access management domain speaks directly to the authentication and credential weaknesses — both the current Studio 5000 session-spoofing technique

and CyberAv3ngers' earlier default-credential exploitation — that have repeatedly given attackers a path into water-sector OT [15]. Utilities and state IT organizations building out the incident-response and vulnerability-management maturity this event demonstrates they need can use AICM's control structure to formalize practices that, in Minnesota, were executed successfully but on an ad hoc, incident-driven basis.

References

[1] BleepingComputer. "Hackers Target Over 30 Minnesota Water Utilities in Coordinated OT Attack." BleepingComputer, July 2026.

[2] Help Net Security. "Coordinated Cyberattack Hits More Than 30 Minnesota Water Utilities." Help Net Security, July 30, 2026.

[3] Tenable. "Minnesota Water Cyber Attack and CISA Advisory AA26-097A: What You Need to Know." Tenable, July 2026.

[4] SecurityWeek. "Dozens of Minnesota Water Utilities Targeted in Coordinated OT Attacks." SecurityWeek, July 2026.

[5] MPR News. "More Than 30 Minnesota Water Systems Targeted in Cyberattack." Minnesota Public Radio, July 29, 2026.

[6] The Hacker News. "Coordinated Cyberattack Targets 30+ Minnesota Water Systems as One Plant Goes Offline." The Hacker News, July 2026.

[7] Cyber Defense Magazine. "Over 30 Minnesota Water Utilities Disrupted in Coordinated Weekend Cyberattack." Cyber Defense Magazine, July 2026.

[8] StateScoop. "Coordinated Cyberattack Disrupts Water Utilities in 30+ Minnesota Communities." StateScoop, July 2026.

[9] SecurityWeek. "CISA Urges Water Sector to Protect OT After Coordinated Attacks on PLCs." SecurityWeek, July 2026.

[10] Tech Times. "Iranian Hackers Exploited Unpatchable PLC Flaw to Breach 30 Minnesota Water Systems." Tech Times, July 29, 2026.

[11] The Register. "Iran-Linked CyberAv3ngers Suspected in Attacks on Minnesota Water Systems." The Register, July 29, 2026.

[12] CBS News. "U.S. Investigating Whether Iran Was Behind Cyberattack on Minnesota Water Systems." CBS News, July 2026.

[13] The Hacker News. "Hikvision and Rockwell Automation CVSS 9.8 Flaws Added to CISA KEV Catalog." The Hacker News, March 2026.

[14] Cloud Security Alliance. "Zero Trust Guidance for Critical Infrastructure." CSA Zero Trust Working Group, 2024.

[15] Cloud Security Alliance. "AI Controls Matrix (AICM) v1.1." CSA, 2026.

[16] Cybersecurity and Infrastructure Security Agency. "IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities (AA23-335A)." CISA, updated December 2024.

[17] U.S. Government Accountability Office. "Critical Infrastructure Protection: Actions Needed to Address Persistent Cybersecurity Threats to the Water and Wastewater Sector." GAO-26-109159, 2026.