MAGNET S2

INTELLIGENCE REPORT

DTG: 260806-1800Z | Geographic Focus: United States (Multi-State)

www.magnethf.com

REPORT IDENTIFICATION

Subject	Coordinated Multi-State Cyberattack Campaign Targeting Water and Wastewater Utility Control Systems
Purpose	Provide MAGNET operators intelligence awareness of an ongoing cyber intrusion campaign against water and wastewater operational technology (OT) systems across multiple U.S. states, and outline readiness and communications posture in the event local support is requested.
DTG	260806-1800Z
Reporting Period	26 July – 06 August 2026
Geographic Focus	United States — confirmed impacts in Minnesota, Michigan, Georgia, South Dakota, and New Jersey; open-source reporting indicates activity in as many as 12 states; Wisconsin issued a precautionary advisory
Precedence	RR – ROUTINE
MagCon Status	**3 – ELEVATED**
Sources	Multiple source reporting from Local, National, and International platforms. See source list.

SUMMARY (BLUF)

Since 26–27 July 2026, malicious cyber actors have compromised internet-exposed programmable logic controllers (PLCs) at water and wastewater utilities beginning in Minnesota, where more than 30 community systems were affected within roughly 48 hours; open-source reporting now places the campaign in as many as 12 states, with Minnesota, Michigan, Georgia, South Dakota, and New Jersey publicly confirmed.

Attackers are targeting Rockwell Automation/Allen-Bradley MicroLogix 1100/1400 controllers, altering IP addresses and passwords to lock operators out of monitoring and control functions, producing pressure loss, communications outages, manual-operations fallbacks, and precautionary boil-water notices at several sites.

No drinking-water contamination has been confirmed, and federal agencies have not issued a formal attribution; multiple officials cite Iran-affiliated actors as the leading suspect while investigators simultaneously assess the possibility that the activity is a false-flag operation designed to mimic Iranian tradecraft.

FBI, EPA, and CISA have issued nationwide advisories directing water and wastewater operators to remove PLCs from direct internet exposure immediately, and separate reporting indicates the campaign exploited a specific software vulnerability for which a vendor fix has since been released.

BACKGROUND

On 7 April 2026, CISA, the FBI, NSA, EPA, DOE, and U.S. Cyber Command's Cyber National Mission Force jointly published Cybersecurity Advisory AA26-097A, warning that Iranian-affiliated actors were exploiting internet-exposed Rockwell Automation/Allen-Bradley PLCs across the Water and Wastewater, Energy, and Government Services sectors.

On 22 July 2026 — four days before the Minnesota intrusions began — the advisory was updated to expand the observed target set to Schneider Electric and Siemens controllers, document exfiltration of PLC project files for the first time, and add detection guidance for manipulation of reusable ladder-logic code modules; the U.S. Department of the Treasury joined as a co-authoring agency.

This is not the first campaign of its kind. In November 2023, actors linked to Iran's IRGC compromised a water utility near Pittsburgh, Pennsylvania using similar techniques against internet-facing Unitronics PLCs (the "CyberAv3ngers" activity), and the U.S. Treasury Department sanctioned that group in February 2024.

The current campaign follows broadly similar tradecraft — internet-facing OT devices reachable with weak, default, or reused credentials — but has affected a substantially larger number of utilities across more states within a compressed timeframe, and against a different equipment model line than the 2023 incidents.

SITUATION

Minnesota

Minnesota IT Services (MNIT) reported that over 30 community water and wastewater systems were affected in a coordinated intrusion over the weekend of 26–27 July. A plant in Braham went offline for approximately two hours. Plymouth lost radio/cellular connectivity to water towers and pump stations. South St. Paul and Maple Plain also had automatic control functions affected; Maple Plain declared a local emergency.

Federal Advisories

In a 30 July joint Public Service Announcement, the FBI and EPA stated that water and wastewater utilities in at least seven states had reported incidents since 27 July involving internet-facing Rockwell Automation/Allen-Bradley MicroLogix 1100/1400 controllers. Actors remotely accessed the devices and changed IP addresses and passwords, causing loss of monitoring and control; the agencies noted that a sufficient pressure drop could theoretically allow untreated groundwater to enter distribution pipes.

CISA separately confirmed a significant increase in threat-actor activity against water-sector PLCs, noted that some utilities had issued boil-water notices and shifted to manual operations, and directed all water and wastewater operators to disconnect these controllers from the internet immediately.

Georgia

The Clayton County Water Authority reported a pump station failure at approximately 0100 hrs on 27 July, causing low or no water pressure for some customers; a precautionary boil-water notice was issued and lifted the following day after clean water-quality testing. Columbus Water Works, in a separate incident the same day, identified and stopped an intrusion attempt with no impact to customers.

Michigan

Michigan's Department of Environment, Great Lakes, and Energy (EGLE) and state police confirmed that nine municipal water systems showed activity consistent with the campaign as of 1 August. All systems continued operating safely with no public-health impact reported.

South Dakota

Rapid City officials reported a cyber incident targeting a wastewater lift station, identified and contained quickly with no impact to drinking water or wastewater operations. The city is working with CISA and other federal partners; a separate, unrelated cyberattack has affected Pennington County government networks since early July.

New Jersey

New Jersey's state cybersecurity office reported that two municipal water systems briefly lost visibility into automated controls on 5 August and shifted to manual operations; there was no disruption to customers, and security measures have since been tightened.

Scope of Reporting

ABC News and CBS News, citing individuals familiar with the investigation, reported on 4–6 August that the campaign has now been identified in at least 12 states, though only five have been publicly confirmed by name (MN, MI, GA, SD, NJ). Wisconsin's state environment agency issued a precautionary advisory to water utilities; no confirmed intrusions have been reported there as of this writing.

Attribution and Political Response

The New York Times and Washington Post, citing officials briefed on the matter, reported on 30–31 July that investigators preliminarily assess the tradecraft and absence of a ransom demand as consistent with Iranian-affiliated activity, while cautioning that the assessment is preliminary and could change, and that investigators have not ruled out a deliberate impersonation of Iranian tactics.

President Trump stated on 31 July that he did not believe Iran was responsible and attributed the incident to poor preparedness by Minnesota's state government. Minnesota Governor Tim Walz responded that multiple states had been affected and cited reductions in federal CISA funding and staffing as a contributing factor; CISA's FY2026 appropriation (~$2.6B) was lower than its FY2025 appropriation (~$2.8B).

Vulnerability and Vendor Guidance

Reporting on 5 August indicated the campaign also exploited a specific vulnerability in widely used utility control software — not solely default-credential exposure — and that a vendor fix has since been issued; utilities nationwide running the same software are being urged to patch, meaning additional affected sites may still be identified.

Rockwell Automation advised customers operating affected MicroLogix 1400 units to power the devices off, remove the battery to force a reset, maintain offline configuration backups, and discontinue direct internet connectivity for these controllers.

Status of Attribution (as of DTG)

As of 6 August, investigators have not made a formal, official attribution determination. Officials describe the false-flag possibility — that a different threat actor deliberately mimicked Iranian tactics, techniques, and procedures to inflame tensions during the ongoing U.S.–Iran conflict — as an active line of investigation rather than background speculation.

Timeline of Known Activity

07 Apr	CISA/FBI/NSA/EPA/DOE/CNMF publish Advisory AA26-097A on Iranian-affiliated PLC exploitation across critical infrastructure.
22 Jul	Advisory AA26-097A updated: scope expanded to Schneider Electric/Siemens PLCs; project-file exfiltration documented; Treasury joins as co-author.
26–27 Jul	Coordinated intrusion affects 30+ community water/wastewater systems across Minnesota over a single weekend.
27 Jul	Clayton County, GA pump station fails; precautionary boil-water notice issued. Columbus Water Works, GA detects and stops a separate intrusion attempt.
30 Jul	FBI/EPA joint PSA and CISA advisory confirm activity in at least seven states; both agencies direct utilities to disconnect PLCs from the internet.
30–31 Jul	NYT/WaPo report preliminary official assessment points toward Iran-affiliated actors; President Trump publicly rejects that attribution and blames Minnesota; Gov. Walz responds, citing multi-state scope and federal cybersecurity funding cuts.
31 Jul	Rapid City, SD reports and contains a cyber incident at a wastewater lift station.
01 Aug	Michigan (EGLE/state police) confirms nine water systems show activity consistent with the campaign.
04–06 Aug	ABC News/CBS News report the campaign has expanded to at least 12 states (5 confirmed by name); Wisconsin issues a precautionary advisory.
05 Aug	New Jersey reports two systems briefly lost automated-control visibility. ABC7 New York reports a specific exploited software vulnerability (fix issued) and confirms the false-flag angle is under active investigation.
06 Aug	CBS News reports no formal attribution determination has been made; assessment remains subject to revision as technical evidence develops.

COMMENTS / ASSESSMENT

This campaign did not require novel intrusion techniques — it succeeded because water utility control systems remained directly reachable from the internet with weak, default, or reused credentials, a vulnerability class that has been publicly flagged by federal agencies for years, most recently in the 22 July update to AA26-097A. The near-simultaneous impact across more than 30 Minnesota utilities suggests the actors likely used automated scanning against a known device fingerprint, or that a number of affected utilities share a common integrator, managed service provider, or telecom pathway that replicated the same exposure across multiple sites; the FBI's PSA itself flags shared third-party network setups as a plausible force multiplier.

Iran-affiliated involvement is assessed as a reasonable working hypothesis given consistent tradecraft with the CyberAv3ngers/IRGC-CEC campaign tracked since 2023 and the timing relative to the 22 July advisory update, but it remains unconfirmed. Investigators are explicitly weighing a false-flag scenario in which a different actor adopted Iranian-style TTPs to inflame U.S.–Iran tensions amid the active conflict. MAGNET reporting and communications should characterize attribution as under investigation and avoid repeating either the Iran attribution or the political attribution exchange between the White House and Minnesota's governor as established fact.

Available reporting indicates the intended or plausible effect has been disruption, confusion, and erosion of confidence in OT reliability rather than deliberate contamination of drinking water, though the FBI has noted that a sufficiently large, sustained pressure drop could theoretically permit untreated groundwater intrusion into distribution piping. The disclosure of an exploited software vulnerability — distinct from simple internet exposure — means the population of at-risk utilities is likely larger than the 12 states currently identified, pending nationwide patch adoption.

Current Assessment

ASSESSMENT CATEGORY	PROBABILITY
Opportunistic Exploitation of Known, Unpatched Internet-Facing OT	**HIGH**
Iranian State-Affiliated Involvement (Unconfirmed)	**MODERATE-HIGH**
Additional Utilities Compromised via Same Software Vulnerability Before Nationwide Patch Adoption	**MODERATE-HIGH**
False-Flag Operation Deliberately Mimicking Iranian TTPs	**LOW-MODERATE**
Deliberate Water Contamination as a Primary Attack Objective	**LOW**

Note: Probability levels reflect currently available open-source reporting only. Federal agencies have made no formal attribution as of the DTG of this report, and this assessment may be revised as additional technical evidence is developed.

INTELLIGENCE GAPS

- Will federal agencies reach and publicly release a formal attribution determination, and on what timeline?
- What is the specific software product/vulnerability referenced in 5 August reporting, and what proportion of U.S. water utilities run the affected version?
- Have investigators found technical evidence either confirming or ruling out a false-flag operation mimicking Iranian TTPs?
- What is the complete list of affected states beyond the five publicly confirmed to date?
- Do any of the affected Minnesota utilities share a common integrator, managed service provider, or remote-access architecture that could explain the near-simultaneous impact?
- Has any utility's water quality been independently retested and confirmed safe following each reported incident, beyond the initial boil-water notice/lift cycle?
- Is there any indication of coordination between this cyber campaign and other hostile activity tied to the ongoing U.S.–Iran conflict?

MITIGATION RECOMMENDATIONS

- Follow official sources only (FBI, CISA, state emergency management) for updates on this campaign; do not repeat unconfirmed attribution or scope figures as fact.
- Identify whether a water or wastewater utility in your area is one your net would support in an emergency, and whether it has reported any impact from this campaign.
- If you have an established point of contact at a local water utility or Emergency Operations Center, a simple readiness check-in is appropriate; do not offer to test, inspect, or access their control systems.
- Keep go-kits and radio setups ready in case a utility needs to fall back on phone, radio, or in-person communication after losing normal OT monitoring or control.
- Review how your local net would relay an official message (e.g., a boil-water notice) accurately and without embellishment or speculation.
- Do not speculate on-air or in writing about attribution; characterize it only as "under investigation" and avoid repeating the Iran attribution or the Trump–Walz political exchange as settled fact.
- Do not share technical details about affected equipment, software, or vulnerabilities beyond what is already public.
- Pass any first-hand report of a local water problem (pressure loss, outage, boil-water notice) to net control with location and time heard, for tracking and verification.
- Use this event as a prompt to review your own home network, radios, and remote-access equipment for weak or default credentials and unnecessary internet exposure.

MAGNET GUIDANCE

This is an awareness and readiness report; MAGNET operators are not expected to access, test, or remediate any utility's control systems. If you work with a local water utility or emergency office, you may share the mitigation guidance in this report with the appropriate technical or emergency management contact.

If normal utility communications or SCADA/HMI monitoring is degraded, MAGNET nets should be prepared to serve as an Alternate or Contingency tier under the local PACE plan for relaying verified situational information between utility, Emergency Operations Center, and public-safety points of contact — not as a Primary channel, and only when requested through established channels.

Any first-hand or credible secondhand report of a local water-system anomaly should be passed to net control with the location and time it was heard, so it can be logged and verified before further dissemination.

Questions or local reports should be routed through the usual MAGNET net control / S2 channel.

SOURCE LIST

[1] FBI/EPA — Joint Public Service Announcement [A1] — Malicious Cyber Actors Targeting Water and Wastewater Sector Internet-Facing PLCs, Causing Operational Disruptions (30 Jul 2026). https://www.fbi.gov/investigate/cyber/alerts/2026/malicious-cyber-actors-targeting-water-and-wastewater-sector-internet--facing-programmable-logic-controllers-causing-operational-disruptions

[2] WaterISAC — CISA Advisory AA26-097A Update Summary [A1] — Summary of the 22 Jul 2026 update to joint Cybersecurity Advisory AA26-097A, Iranian-Affiliated Cyber Actors Exploit PLCs Across U.S. Critical Infrastructure. https://www.waterisac.org/tlpclear-cisa-updates-iranian-affiliated-plc-targeting-advisory-aa26-097a

[3] City of Rapid City, SD — Official Statement [A1] — Municipal government press release on the cyber incident affecting a wastewater lift station. https://www.rcgov.org/rapid-city-news-room/city-of-rapid-city-experiences-cyber-incident-to-lift-station-15645.html

[4] CBS News [B2] — At least 12 states report cyberattacks on water systems possibly linked to Iran-backed hackers, sources say. https://www.cbsnews.com/news/more-states-water-systems-cyberattacks-iran-backed-hackers/

[5] NBC News [B2] — Hackers targeted municipal water systems in 7 states this week, FBI says. https://www.nbcnews.com/tech/security/hackers-targeted-municipal-water-systems-7-states-week-fbi-says-rcna590210

[6] ABC News [B2] — Trump blames Minnesota governor, not Iran, for cyberattacks on the state's water systems. https://abcnews.com/Politics/trump-blames-minnesota-governor-iran-cyberattacks-states-water/story?id=135266259

[7] CNN Politics [B2] — Sweeping cyberattack on water systems in multiple states has U.S. officials on edge; false-flag concerns noted. https://www.cnn.com/2026/07/31/politics/sweeping-cyberattack-us-water-systems

[8] CNN Politics [B2] — Why U.S. water systems are vulnerable to foreign cyberattacks — Rapid City and Clayton County detail (06 Aug 2026). https://edition.cnn.com/2026/08/06/politics/why-us-water-systems-are-vulnerable-to-foreign-cyberattacks

[9] Axios [B2] — The number of states targeted in cyberattacks on water systems has jumped to 12. https://www.axios.com/2026/08/04/water-cyberattacks-us-iran

[10] The Record (Recorded Future News) [B2] — Cyberattacks on water systems expand to 12 states as South Dakota, Georgia announce incidents. https://therecord.media/iran-cyberattacks-water-treatment

[11] CyberScoop [B2] — Trump blames Minnesota for cyberattacks on water sector, drawing pushback; WaterISAC comment on attribution alignment. https://cyberscoop.com/trump-blames-minnesota-water-cyberattacks-iran/

[12] ABC News [C3] — At least 12 states face cyberattacks on their water systems, sources say. https://abcnews.com/US/12-states-face-cyberattacks-water-systems-sources/story?id=135348482

[13] ABC7 New York [C3] — New Jersey water utilities targeted; sourcing on the exploited software vulnerability, vendor fix, and false-flag investigation angle. https://abc7ny.com/post/new-jersey-water-utilities-targeted-cyberattacks-widely-believed-linked-iran/19629579/

[14] NBC News [C3] — Iran likely behind cyberattacks on U.S. water systems, sources say. https://www.nbcnews.com/tech/security/iran-likely-cyberattacks-us-water-systems-sources-say-rcna590756

[15] The Hacker News [C3] — Coordinated cyberattack targets 30+ Minnesota water systems as one plant goes offline. https://thehackernews.com/2026/07/coordinated-cyberattack-targets-30.html

Submit reports through established MAGNET situational awareness channels. To Learn More About MAGNET, Visit www.MAGNETHF.COM