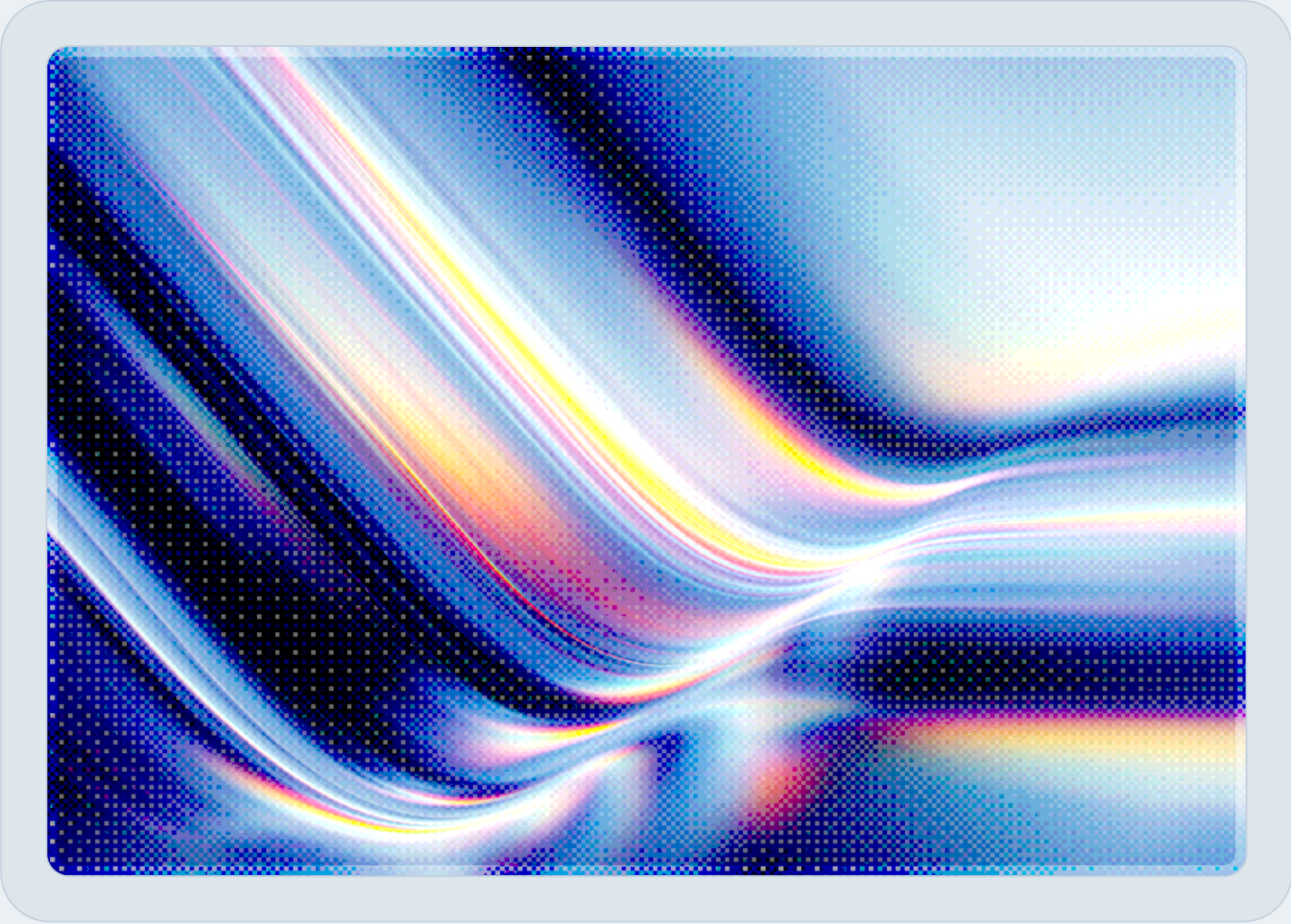
CSAI Foundation | Cloud Security Alliance

Exposed Rockwell PLCs Fuel Ongoing Water Utility Attacks

2026-08-08

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Key Takeaways

An internet-wide scan by Forescout's Vedere Labs, published August 6, 2026, found 4,407 internet-facing Rockwell Automation and Allen-Bradley programmable logic controllers (PLCs) exposed on port 44818 (EtherNet/IP), with 2,844 of them, roughly 65 percent, located in the United States [1][2]. Twenty-two of those exposed controllers sit in cities where water and wastewater utilities have reported cyberattacks since late July 2026, and 19 of the 22 appear vulnerable to CVE-2017-16740, a nine-year-old buffer overflow in MicroLogix 1400 controllers that Rockwell patched in 2017 [1][3]. The FBI and Environmental Protection Agency (EPA) confirmed on July 30 that malicious actors were targeting internet-exposed PLCs at water and wastewater facilities in at least seven states, a number that grew to 12 or more as additional utilities reported incidents through early August [4][5]. In the incidents Forescout documented in detail, intruders were largely walking through the front door, changing IP addresses and resetting passwords on controllers that were never supposed to be reachable from the public internet in the first place, rather than exploiting a software flaw [1][6]. Not every confirmed incident in the current wave has a publicly disclosed intrusion vector, however; officials in Braham, Minnesota, for instance, have attributed a two-hour outage at their water plant to a cyberattack on the facility's operating controls without specifying how the intruders gained access [6][9]. The pattern connects a long-standing OT exposure problem, one Rockwell has warned customers about since 2018, to real-world operational disruptions including pressure loss and flooding risk at drinking water systems [2][6].

Background

Rockwell Automation's MicroLogix and CompactLogix families of PLCs are widely deployed across U.S. water and wastewater treatment plants to manage pumps, valves, chlorination systems, and water tower levels. Many small and mid-sized utilities connect these controllers to cellular routers for remote monitoring and maintenance, a practice that keeps staffing costs low but frequently leaves the underlying EtherNet/IP or Modbus TCP interface reachable from the open internet [1][6]. Rockwell Automation has advised customers since at least 2018 not to place these controllers directly on the public internet, yet Forescout's scan found the exposure has persisted for years: internet-facing Rockwell/Allen-Bradley controllers peaked at 7,814 devices in March 2020 and have declined only 47 percent since, to roughly 4,169 devices by June 2026 and 4,407 by early August [2][6]. Of the U.S.

devices Forescout identified, about 70 percent connect through cellular routers on mobile carrier networks, and MicroLogix 1400 accounts for half of all exposed devices, followed by CompactLogix 1769 at 22 percent and MicroLogix 1100 and ControlLogix 5590 at roughly 8 percent each [1][2].

The current wave of incidents began the evening of July 26, 2026, when attackers compromised PLCs at water systems across Minnesota; Minnesota IT Services publicly disclosed the resulting coordinated cyberattack, which affected more than 30 municipal water systems statewide, on July 27-28 [3][6]. The cities of Plymouth, South St. Paul, Maple Plain, and Braham confirmed operational impacts: Braham reported that a cyberattack against its computerized operating controls shut down the well and water treatment plant for roughly two hours, while in Plymouth attackers disconnected cellular-connected equipment at two water towers and 14 sewer lift stations [6][9][10]. The FBI and EPA issued a joint public service announcement on July 30 warning that cyber actors were targeting internet-facing PLCs, specifically naming MicroLogix 1100 and 1400 series controllers, at water and wastewater facilities across at least seven states, with degraded operations including pressure loss and flooding reported at some sites [4][3]. By early August, utilities in 12 or more states, including Michigan, South Dakota, and Georgia, had reported similar incidents to federal authorities, and some public reporting has raised the possibility of an Iran-linked operational technology campaign, though the Minnesota incidents and the broader multistate activity have not been formally attributed to a named threat actor as of this writing [3][7].

Security Analysis

Forescout's scan matters less for what it reveals about any single attacker than for what it confirms about the underlying attack surface. The scale of the exposure, more than 4,000 devices spread across hundreds of individual operators, suggests a systemic problem rather than isolated misconfiguration, though this note cannot rule out that any individual utility's exposure reflects local factors rather than a sector-wide pattern. The 22 exposed controllers found in cities already hit by attacks represent a small fraction of the 4,407 total, meaning the vast majority of exposed PLCs identified in this research have not yet been targeted; the available scan data does not identify any configuration difference between those targeted devices and the broader exposed population, however, which suggests the remainder may carry similar risk. Nineteen of the 22 controllers tied to attacked cities share the same mobile carrier network, and 19 of 22 appear vulnerable to CVE-2017-16740, a stack-based buffer overflow in MicroLogix 1400 Series B and C running firmware 21.002 or earlier that Rockwell's advisory rates 8.6 on the CVSS scale and that CISA's ICS-CERT confirmed could enable remote code execution [1][8]. Exploiting that flaw requires Modbus TCP to be enabled on the target device, and Forescout could not confirm whether the affected controllers in the current campaign had that service active, so the presence of the vulnerability should be read as an indicator of unpatched, poorly maintained infrastructure rather than proof that this specific flaw was the intrusion vector [1][2].

The technique documented in Forescout's research is more mundane than a zero-day exploit: in the cases researchers could examine, intruders logged into internet-reachable controllers, in some cases using default or weak credentials, and changed IP addresses and passwords to lock operators out of their own equipment [1][6]. Not every confirmed incident in the current wave fits that description; public disclosures for Braham, Minnesota, for example, describe a cyberattack against the plant's operating controls without specifying an intrusion vector [6][9]. Even so, the pattern Forescout observed echoes concerns CISA and water-sector information-sharing organizations have raised previously about default credentials and unsegmented remote access, though this note has not independently verified a multi-year trend across the sector. Forescout also identified secondary exposure indicators around these same utilities, including expired TLS certificates, abandoned remote-access hostnames, and forgotten servers, one of which had served nothing but a default IIS placeholder page since 2019, all pointing to incomplete asset inventories that likely extend well beyond the PLCs themselves [2][6]. GAO has documented that staffing shortages and resource constraints leave many smaller water utilities without the in-house capacity to adopt cybersecurity best practices even when free federal resources are available [11], and that dynamic compounds the risk here: the combination of internet-facing legacy controllers, cellular connectivity with no network segmentation, and years-old unpatched firmware creates conditions in which a single opportunistic actor, regardless of sophistication, can achieve operational impact at scale. Forescout characterized the observed activity as "opportunistic, at-scale exploitation" rather than a targeted, sophisticated campaign [3][1]. That characterization is itself the more concerning finding, in this note's assessment, because it suggests the barrier to disrupting a U.S. water utility is currently quite low.

Recommendations

Immediate Actions

Water and wastewater utilities operating Rockwell Automation or Allen-Bradley PLCs should immediately verify whether any controller, cellular gateway, or remote-access endpoint is reachable from the public internet, starting with port 44818 (EtherNet/IP) and Modbus TCP, and remove any direct exposure found. Utilities should force a credential reset on every internet-facing or remotely accessible controller, replacing default or long-unchanged passwords, and confirm firmware on any MicroLogix 1400 Series B or C device has been upgraded to revision 21.003 or later to close CVE-2017-16740 [8]. Organizations should also inventory cellular-connected OT assets specifically, since roughly 70 percent of the U.S. devices Forescout found were reachable through mobile carrier networks rather than fixed internet connections, a path that is easy to overlook in traditional network scans [1][2].

Short-Term Mitigations

Utilities should route all remote access to PLCs through a dedicated secure remote access gateway that mediates and logs every session, rather than allowing direct inbound connections to the controller itself, and should migrate cellular gateways onto private access point names (APNs) or VPN tunnels rather than leaving them addressable on the public carrier network [2]. Network segmentation between OT and IT environments, combined with allowlisting for port 44818 and Modbus TCP traffic, will reduce the chance that a compromised IT asset or an internet scan can reach the control layer directly. Utilities should also conduct a broader asset audit to catch the kind of secondary exposure Forescout identified, expired certificates, orphaned remote-access hostnames, and forgotten servers, since these often mark the entry points that formal PLC inventories miss [2][6].

Strategic Considerations

The persistence of this exposure eight years after Rockwell first warned customers not to connect these controllers directly to the internet, and nine years after CVE-2017-16740 was patched, indicates that technical guidance alone has not been sufficient to change practice across a sector composed largely of small, resource-constrained utilities [8][6]. Federal support, whether through CISA's regional cybersecurity advisors, EPA technical assistance programs, or state-level grant funding, will likely need to underwrite both the initial remediation and the ongoing monitoring that many utilities cannot otherwise staff. Utilities and their vendors should also treat cellular and remote-access gateways as a first-class part of the OT attack surface in future risk assessments, since this incident illustrates that convenience-driven remote connectivity, not sophisticated exploitation, remains the dominant path into critical water infrastructure in the incidents documented to date.

CSA Resource Alignment

CSA's Zero Trust Guidance for Critical Infrastructure is among CSA's most directly applicable resources for the remediation this incident calls for. It offers a five-step roadmap for applying Zero Trust principles specifically to OT and ICS environments, addressing the architectural differences, legacy protocols, and availability constraints that distinguish water-sector control systems from conventional IT networks, precisely the gap that allowed thousands of Rockwell controllers to remain internet-facing for years without compensating access controls. Utilities implementing the immediate and short-term mitigations above, secure remote access gateways, network segmentation, and private APN or VPN paths for cellular gateways, are effectively executing the early stages of that roadmap. CSA's newer Zero Trust Guidance for Achieving Operational Resilience extends that roadmap into enterprise-wide resilience

planning, which bears directly on the Strategic Considerations above: this incident shows how a single access-control gap, replicated across hundreds of utilities running the same vendor equipment, can produce coordinated, multistate operational disruption rather than an isolated outage.

CSA's State of ICS Security in the Age of Cloud research report examines the benefits of applying cloud computing to ICS/OT environments, a relevant complement to this incident given that Forescout's findings stem from external, internet-wide asset discovery rather than utilities' own internal visibility. The exposure and asset-inventory gaps this campaign has surfaced, including forgotten servers and expired certificates dating back to 2019, are consistent with the visibility challenges the report describes.

For organizations building a shared technical vocabulary around this incident, CSA's Cloud Industrial Internet of Things (IIoT) - Industrial Control Systems Security Glossary defines the IIoT and ICS terminology referenced throughout vendor advisories and federal alerts on this topic. More broadly, the AI Controls Matrix (AICM v1.1) remains the standing reference for organizations layering AI-driven anomaly detection or automated response onto OT environments, though this incident itself is a conventional access-control failure rather than an AI-specific one.

References

[1] The Hacker News. "Over 4,400 Rockwell PLCs Exposed Online, 22 Found in Water Attack Cities." The Hacker News, August 6, 2026.

[2] Forescout Vedere Labs. "OT Security Analysis: Exposed Devices Attacked in US Water Systems." Forescout, August 2026.

[3] CyberScoop. "Despite federal warnings, thousands of U.S. industrial controllers used in water systems remain exposed online." CyberScoop, August 6, 2026.

[4] NBC News. "Hackers targeted municipal water systems in 7 states this week, FBI says." NBC News, July 31, 2026.

[5] Industrial Cyber. "FBI and EPA warn hackers target internet-connected PLCs at US water utilities, leading to operational disruptions." Industrial Cyber, July 2026.

[6] LevelBlue. "Review of the July 2026 Cyberattacks Against U.S. Water and Wastewater Systems." LevelBlue SpiderLabs Blog, August 2026.

[7] Fortune. "Iranian hackers and America's Achilles heel on water: default passwords." Fortune, August 5, 2026.

[8] CISA. "Rockwell Automation Allen-Bradley MicroLogix 1400 Controllers (ICSA-18-009-01)." Cybersecurity and Infrastructure Security Agency, January 2018.

[9] CBS Minnesota. "'Coordinated cyberattack' targeted 30-plus Minnesota water systems in 48 hours, MNIT says." CBS News Minnesota, July 28, 2026.

[10] Governing. "Troubled Waters: Minnesota Cities Weather Cyber Attack." Governing, July 31, 2026.

[11] U.S. Government Accountability Office. "Critical Infrastructure Protection: EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems (GAO-24-106744)." U.S. GAO, August 2024.

