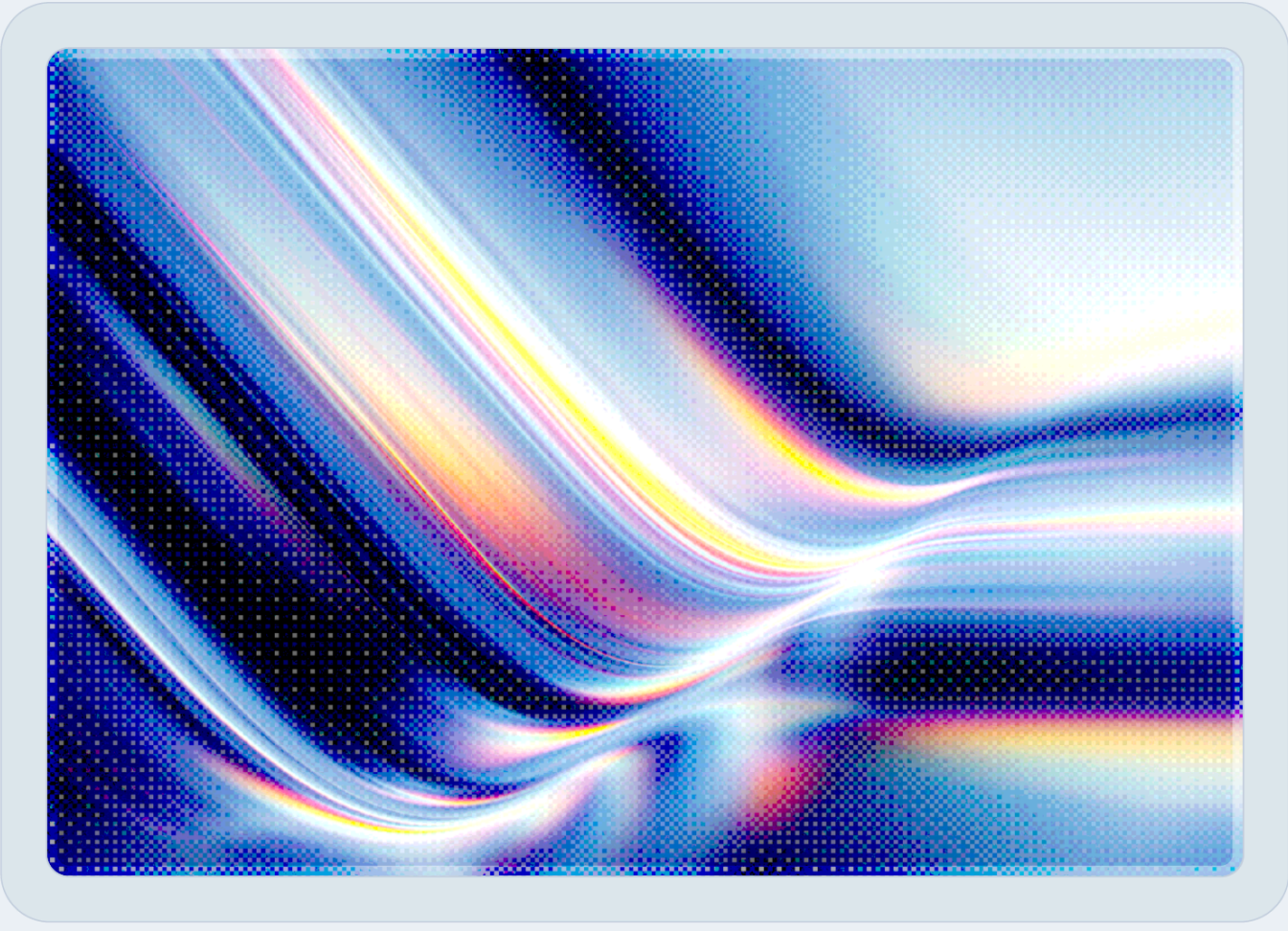
CSAI Foundation | Cloud Security Alliance

Exposed Rockwell PLCs at Water Utilities: Security Implications and Guidance

2026-08-07

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Key Takeaways

A Shodan-based exposure scan conducted by Forescout's Vedere Labs on August 3, 2026 identified 4,407 internet-facing Rockwell Automation and Allen-Bradley programmable logic controllers (PLCs) worldwide, with 2,844 of them located in the United States [1][3]. Twenty-two of the exposed controllers sit in cities already confirmed as victims of the water-sector attacks that began in late July 2026, and 19 of those 22 devices run firmware vulnerable to a 2017 remote code execution flaw, CVE-2017-16740, that Rockwell patched nine years ago [1][3]. The finding demonstrates that the exposure problem underlying the current campaign is broader than the confirmed incident list: thousands of similarly configured controllers remain reachable from the open internet regardless of whether an attacker has touched them yet.

The active campaign, first reported on July 27, 2026, disrupted water and wastewater operations in at least 12 U.S. states, with the most severe impacts occurring in Minnesota, where more than 30 municipal systems were affected and at least four cities publicly confirmed operational disruption [1][2][4]. The FBI and EPA issued a joint public service announcement on July 30 describing attackers who remotely changed IP addresses and passwords on exposed MicroLogix controllers to lock operators out of their own systems, in some cases causing pressure loss and flooding conditions with the potential to allow untreated groundwater into distribution pipes [1][2][4]. The U.S. government has attributed the broader campaign to CyberAv3ngers, a persona associated with Iran's Islamic Revolutionary Guard Corps Cyber Electronic Command (IRGC-CEC), under an updated joint advisory, AA26-097A [5]. Forescout researchers caution, however, that the exposure they documented reflects opportunistic, at-scale scanning of any reachable device rather than evidence that every exposed controller has been individually targeted by a sophisticated actor [2].

This note summarizes the exposure data, situates the current campaign within a multi-year pattern of PLC-targeted attacks on the U.S. water sector, and provides prioritized guidance for water utilities and other critical infrastructure operators running internet-reachable Rockwell equipment.

Background

A Recurring Target: Internet-Exposed PLCs in the Water Sector

The water and wastewater sector has been a persistent target for PLC-focused intrusions since at least 2023. Analysts attribute this pattern in part to IT staffing constraints at small and mid-sized utilities, which often lack the resources to maintain network segmentation between engineering equipment and the public internet, and to utilities' reliance on cellular modems as a common, low-cost way to monitor geographically dispersed pump stations and lift stations. In November 2023, CyberAv3ngers compromised a Unitronics Vision Series PLC at the Municipal Water Authority of Aliquippa, Pennsylvania, taking advantage of a device that was directly internet-accessible and still running default credentials [6] [7]. CISA, the FBI, and international partners subsequently documented that the group compromised at least 75 Unitronics PLCs across the United States, the United Kingdom, Israel, and Ireland between October 2023 and January 2024 through the same default-credential technique, in an advisory tracked as AA23-335A [6].

The group's tradecraft evolved over the following two years. Security researchers observed a mid-2024 shift toward IOCONTROL, a custom Linux-based malware platform built to target routers, PLCs, human-machine interfaces, and fuel management systems using MQTT-over-TLS command-and-control channels [5][8]. By March 2026, CISA and partner agencies reported that CyberAv3ngers-linked actors had pivoted away from default-credential abuse and toward exploitation of CVE-2021-22681, a critical authentication bypass (CVSS 9.8) affecting Rockwell Automation Logix controllers for which no vendor patch exists, alongside two additional vulnerabilities in ControlLogix communication modules, CVE-2023-3595 and CVE-2024-6242 [5][9]. That shift in target platform, from Unitronics hardware to the more widely deployed Rockwell/Allen-Bradley product line, likely broadened the population of U.S. critical infrastructure operators exposed to this threat actor.

The July 2026 Campaign

The current wave began on July 26–27, 2026, when Minnesota IT Services identified a coordinated cyberattack affecting more than 30 water systems statewide [4]. Braham, Plymouth, South St. Paul, and Maple Plain each confirmed operational impact; in Braham, the intrusion disabled computerized operating controls and temporarily shut down the city's well and water treatment plant, while Plymouth's IT division disconnected cellular equipment serving two water towers and 14 sewer lift stations to contain the incident [4]. Within days, the FBI and EPA confirmed related incidents in Michigan, where nine systems were affected, and in South Dakota and Georgia, bringing the total footprint to at least 12 states [1][2][4]. CISA updated advisory AA26-097A on July 22, 2026 to add detection guidance for malicious

changes to reusable code modules within Rockwell PLC programs; the authoring agencies for that advisory include the FBI, CISA, NSA, EPA, the Department of Energy, U.S. Cyber Command, and the Treasury Department [5].

Across the confirmed incidents, the attackers' methodology has been consistent: rather than deploying custom malware, they modify controller logic or remotely change IP addresses and passwords on internet-exposed MicroLogix 1100 and 1400 PLCs, denying legitimate operators visibility into and control over their own equipment [1][2][4]. This is a comparatively low-effort technique that does not require a zero-day exploit against a device that is already reachable without authentication, which helps explain why Forescout's broader exposure scan—independent of the confirmed victim list—found so many similarly configured, similarly reachable devices.

Security Analysis

What Forescout's Scan Found

Querying Shodan for hosts exposing port 44818, the TCP port used for EtherNet/IP communications, Forescout's Vedere Labs team identified 4,407 internet-facing Rockwell Automation and Allen-Bradley controllers on August 3, 2026 [1][3]. Sixty-five percent of the exposed population sits in the United States, with Canada accounting for 12 percent and Spain for 3 percent [3]. Forescout's own trend data shows a more complicated trajectory than a single point-in-time comparison suggests: global exposure fell from 7,814 devices in March 2020 to a low of 4,169 in June 2026—a 47 percent decline—before rising back to 4,407 by the August 3 scan this note otherwise relies on, a two-month increase the underlying report does not explain [3]. Measured against the original 2020 baseline, the August count still represents a net 43.6 percent reduction, but the recent uptick complicates any claim that exposure is on a steady downward trajectory.

Device-model data from the scan shows MicroLogix 1400 controllers accounting for half of all exposed assets, followed by CompactLogix 1769 units at 22 percent, and MicroLogix 1100 and ControlLogix 5590 controllers each at 8 percent [3]. The FBI and EPA's July 30 advisory specifically named MicroLogix 1100 and 1400 as the models targeted in the confirmed water-sector incidents, so the overlap between these two lines and more than half of Forescout's global exposure count is consistent with elevated near-term risk, though a global exposure scan cannot by itself confirm that every one of those devices faces active targeting [1][3][4].

Table 1 summarizes the exposure and vulnerability data Forescout reported for the subset of hosts located in cities already affected by the current campaign, along with the corrected exposure-trend figures discussed above.

Metric	Value	Source
Globally exposed Rockwell/Allen-Bradley controllers (port 44818)	4,407	Forescout, Aug. 3, 2026 scan [1][3]
Exposed controllers located in the U.S.	2,844 (65%)	Forescout [1][3]
Exposed hosts in cities already hit by the campaign	22	Forescout [1][3]
Of those, running firmware vulnerable to CVE-2017-16740	19 (86%)	Forescout [1][3]
U.S.-based exposed controllers reachable via cellular carrier networks	Over 70%	Forescout [3]
Global exposure low point, June 2026 (down from 7,814 in March 2020)	4,169 devices (47% decline)	Forescout [3]
Net reduction from March 2020 to the August 2026 scan (7,814 → 4,407)	43.6%	Forescout [3]

Two Distinct Vulnerability Chains at Work

It is important to distinguish between the two vulnerability classes implicated in this story, since they point to different remediation paths. The first, CVE-2017-16740, is a Modbus TCP buffer overflow affecting MicroLogix 1400 Series B and C controllers running firmware 21.002 or earlier; Rockwell assigned it a CVSS score of 8.6 and shipped a fix, firmware revision 21.003, in December 2017 [1][10]. Because this is a vulnerability with an available patch, its continued prevalence—affecting 86 percent of the 22 exposed hosts Forescout examined in already-attacked cities—is suggestive of patch and firmware-update lag in at least this subset of the water sector, rather than a gap in vendor remediation, though the sample is too small to generalize to the sector as a whole [1][3].

The second vulnerability chain, centered on CVE-2021-22681 (the Logix controller authentication bypass CISA added to its Known Exploited Vulnerabilities catalog in March 2026 following confirmed CyberAv3ngers exploitation), has no vendor patch at all; Rockwell's guidance instead calls for compensating architectural controls such as network isolation and monitoring for unauthorized logic changes [5][9]. The two additional CVEs named in the updated AA26-097A advisory, CVE-2023-3595 and CVE-2024-6242, affect ControlLogix communication modules and the Trusted Slot feature respectively, and together with CVE-2021-22681 describe a persistent-access and logic-manipulation capability against Rockwell's higher-end Logix product line that is separate from, though related to, the MicroLogix exposure Forescout measured [5][9]. Utilities running any Rockwell Logix or MicroLogix equipment should treat firmware currency and authentication-bypass exposure as two separate items on their remediation checklist, since patching alone does not close the unpatched authentication bypass.

Attribution Is Confirmed for Some Incidents, Uncertain for the Broader Exposure Population

The U.S. government's attribution of the confirmed water-sector intrusions to CyberAv3ngers, and by extension to IRGC-CEC, rests on TTPs and indicators of compromise documented in advisory AA26-097A, and reflects a pattern, consistent with the incidents described in this note, of disruptive rather than destructive effect [5]. That attribution, however, applies specifically to the confirmed victim incidents in Minnesota, Michigan, South Dakota, and Georgia. Forescout's Sai Molige, commenting on the broader 4,407-device exposure count, noted that the pattern more closely resembles opportunistic, at-scale exploitation of anything reachable on the internet than a series of individually selected targets, which is a meaningfully different risk model for utility defenders [2]. In practice, both framings matter: a utility operating an exposed, vulnerable MicroLogix controller faces risk both from a possible continuation of the confirmed nation-state-linked campaign and, independently, from opportunistic scanning and exploitation by any actor capable of running the same freely available reconnaissance and exploitation tooling.

Remote Access Architecture Is the Common Failure Mode

A consistent thread across the Forescout data and the FBI/EPA advisory is the role of cellular remote access. Over 70 percent of the U.S.-based exposed controllers in Forescout's scan connect through cellular routers on major mobile carrier networks [3]. Press reporting on a separate July 30, 2026 Censys snapshot found that Verizon Business, AT&T Mobility, and T-Mobile USA together account for 59 percent of exposed hosts [1]. Cellular modems are attractive to utilities precisely because they provide connectivity to remote pump stations and lift stations without requiring wired infrastructure, but when deployed without a private access point name (APN), VPN tunnel, or equivalent access-control layer,

they function as an unauthenticated bridge from the public internet directly to plant-floor control logic [3]. Forescout also flagged expired certificates, unrenewed remote-access hostnames, and abandoned vendor or integrator servers as contributing factors that expand the attack surface beyond the currently commissioned equipment inventory [2][3].

Recommendations

Immediate Actions

Water utilities and other critical infrastructure operators running Rockwell Automation or Allen-Bradley PLCs should immediately inventory every controller reachable from the public internet, giving priority to devices exposing port 44818 (EtherNet/IP) or Modbus TCP, and should remove direct internet exposure for any controller that does not require it for legitimate remote operations [1][3]. For MicroLogix 1400 controllers still running firmware 21.002 or earlier, upgrading to firmware 21.003 or later closes CVE-2017-16740 and should be treated as an urgent action given that 86 percent of the exposed hosts Forescout found in already-attacked cities remain on vulnerable firmware [1][10]. Utilities should also cross-reference their own asset inventories against the indicators of compromise published in CISA advisory AA26-097A, particularly the July 22, 2026 update addressing malicious modifications to reusable Rockwell PLC code modules [5].

For controllers accessed via cellular modem, organizations should confirm whether the connection routes through a private APN or an equivalent access-controlled path rather than a public-facing cellular IP address, since Forescout identified this configuration in over 70 percent of the U.S. exposure it measured [1][3]. Any account or credential associated with remote PLC access should be reviewed for default or shared passwords, consistent with the technique CyberAv3ngers used in its original 2023–2024 Unitronics campaign [6][7].

Short-Term Mitigations

Because CVE-2021-22681 has no vendor patch, utilities running Rockwell Logix controllers should implement the compensating controls CISA and Rockwell recommend: network segmentation isolating engineering and SCADA networks from IT and internet-facing networks, monitoring for unauthorized changes to controller logic and configuration, and physical mode-switch settings that prevent remote logic modification where operational requirements allow [5][9]. Organizations should deploy allowlisting on port 44818 and Modbus TCP so that only known, authorized engineering workstations can

communicate with controllers, and should audit VPN configurations, TLS certificates, and remote-service hostnames associated with PLC access for currency and continued ownership, since abandoned infrastructure was cited as a contributing exposure factor [2][3].

Utilities should also maintain current, offline copies of controller logic and configuration to support rapid recovery in the event that an attacker modifies or locks operators out of a device. Such backups likely would have shortened recovery time in incidents like Braham's, where operators lost control of the treatment plant's operating controls, though the cited reporting does not quantify recovery-time impact directly [1][2]. Where feasible, multifactor authentication should be enforced for any remote access path to engineering equipment, and unused management protocols such as SNMP should be disabled on internet-reachable devices [3].

Strategic Considerations

The 43.6 percent net reduction in global Rockwell PLC exposure since 2020 is consistent with sustained attention to this problem producing some results, though Forescout's own data shows exposure has ticked back up since its June 2026 low, and the source does not isolate awareness campaigns or utility modernization as the specific cause of the longer-term decline. The persistence of over 4,400 exposed controllers suggests that voluntary remediation alone may not be closing the gap; among the 22 exposed hosts Forescout found in already-attacked cities, 19 remain on vulnerable firmware, though this sample is too small to establish that victim cities disproportionately overlap with vulnerable devices sector-wide [1][3]. Sector-level coordination bodies, including WaterISAC and state drinking water primacy agencies, are positioned to drive systematic exposure reduction campaigns analogous to the CISA-led efforts following the 2023 Aliquippa incident, and utilities should treat participation in such coordinated remediation efforts as a standing operational priority rather than a one-time response to a specific advisory. Because the underlying exposure problem spans multiple vulnerability classes, vendors, and threat actors—both a confirmed nation-state-linked campaign and opportunistic mass scanning—utilities should adopt architecture-level controls (segmentation, private remote access, monitoring) that reduce risk regardless of which specific actor or CVE is exploited next.

CSA Resource Alignment

CSA's **Zero Trust Guidance for Critical Infrastructure** provides a directly applicable framework for the remote-access and segmentation failures documented in this note [11]. Its five-step Zero Trust implementation process—defining the protect surface, mapping operational flows, and building policy enforcement around OT assets—maps closely onto the specific gap Forescout identified: cellular-

connected PLCs reachable from the public internet without a private APN, VPN, or equivalent policy enforcement point in between. The guidance's emphasis on treating remote access to OT/ICS environments as a defined, monitored transaction flow rather than an open connection directly addresses the architecture failure common to the confirmed July 2026 incidents.

CSA's **State of ICS Security in the Age of Cloud** offers relevant historical and analytical context, documenting a consistent pattern of ICS/SCADA compromises—including prior water-sector incidents—driven by internet-connected legacy equipment and limited OT visibility [12]. Its analysis of the risk introduced by direct internet connections to industrial control equipment, and of the resourcing constraints that lead smaller operators to accept that risk, is directly relevant to understanding why water utilities in particular continue to appear in exposure scans years after the 2023 Aliquippa incident first drew national attention to the problem.

Finally, CSA's **AI Controls Matrix (AICM) v1.1** was designed for AI system governance rather than OT/ICS environments, and its applicability here is secondary. Utilities that also operate AI-enabled monitoring, anomaly-detection, or control systems alongside their Rockwell equipment may find its IAM and asset-inventory control objectives a useful supplementary reference for extending access-management discipline across converged IT/OT/AI environments, though it should not be treated as a primary framework for the exposure problem this note addresses [13].

References

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

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

[3] Forescout Vedere Labs, "OT Security Analysis: Exposed Devices Attacked in US Water Systems," August 5, 2026.

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

[5] Cybersecurity and Infrastructure Security Agency, "Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure (AA26-097A)," originally published April 7, 2026, updated July 22, 2026.

[6] Cybersecurity and Infrastructure Security Agency, "IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities (AA23-335A)," December 1, 2023, updated December 2024.

[7] SecurityWeek, "Hackers Hijack Industrial Control System at US Water Utility," November 2023.

[8] Tenable, "CyberAv3ngers: FAQ About the Iran-Linked Threat Group Targeting U.S. Critical Infrastructure," 2026.

[9] Cybersecurity and Infrastructure Security Agency, National Vulnerability Database, "CVE-2021-22681," authentication bypass in Rockwell Automation Logix controllers, added to the CISA Known Exploited Vulnerabilities catalog March 2026.

[10] Cybersecurity and Infrastructure Security Agency, "Rockwell Automation Allen-Bradley MicroLogix 1400 Controllers (ICSA-18-009-01)," CVE-2017-16740, January 2018.

[11] Cloud Security Alliance, "Zero Trust Guidance for Critical Infrastructure," 2024.

[12] Cloud Security Alliance, "State of ICS Security in the Age of Cloud," 2022.

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

This research note was produced by the Cloud Security Alliance AI Safety Initiative as a point-in-time analysis based on publicly available information as of August 7, 2026. It is intended to inform security professionals and critical infrastructure operators about emerging threats and does not constitute legal, compliance, or audit guidance.