Limehawk, LLC
Knoxville, TN
limehawk.io

FOR IMMEDIATE RELEASE
August 1, 2026

Limehawk Urges Utilities to Take Control Systems Off the Internet After FBI–EPA Alert

The agencies report active attacks on internet-facing controllers at water utilities in at least seven states, with pressure loss and flooding reported.

KNOXVILLE, Tenn., Aug. 1, 2026 — Limehawk, LLC, a Knoxville managed IT services provider, today urged water and wastewater utilities and small industrial operators to remove programmable logic controllers (PLCs) from direct internet exposure. The call follows a public service announcement the Federal Bureau of Investigation and the Environmental Protection Agency issued July 30, 2026.

According to the alert, malicious cyber actors have attacked internet-facing Rockwell Automation/Allen-Bradley MicroLogix 1100 and 1400 series PLCs since July 27, 2026. Water and wastewater utilities in at least seven states have reported incidents to the FBI. After the actors gained remote access, they changed device IP addresses and set new passwords. Operators lost the ability to monitor and control connected equipment. Reported operational effects include loss of pressure and flooding. At least one organization found unauthorized changes to PLC project files across several sites.

“These attacks did not require advanced tools,” said Corey Watson, Managing Member of Limehawk. “The targets were controllers that sat directly on the public internet, often behind a cellular modem, with weak or default credentials. If a device you rely on is reachable from the internet, assume someone is scanning it today. Put a secure gateway in front of it, set strong unique passwords, and lock the key switch back into run mode.”

The FBI has observed this activity only on the named Rockwell models. The agencies advise operators of other PLC brands to take the same precautions.

Background: What Is Known So Far

The federal alert. The FBI and EPA published the PSA on July 30, 2026 (Alert Number I-073026-PSA) [1][2]. The agencies report that similar network setups supplied by third-party providers appeared across multiple victims. This similarity may let the attackers repeat the same access method against several utilities at once [1]. Per the PSA, the severity of each compromise depended on four factors: whether the PLC monitored or controlled equipment, the device model (1100 versus 1400), the function the device supported, and the utility's ability to switch to manual operations [2].

Minnesota. A coordinated campaign on July 26–27, 2026 disrupted water and wastewater operations in more than 30 Minnesota communities [3][4]. Identified municipalities include Braham (population about 1,700), Plymouth (population about 80,000), South St. Paul, Maple Plain, and Eagan [4][5]. In Braham, the disruption temporarily left the community dependent on water stored in its tower [4]. Reported consequences across the campaign included loss of water pressure, flooding, communications outages, boil-water notices, and forced manual operation [4].

Other confirmed states. Michigan reported altered settings on wastewater equipment in a small number of communities, with no threat to drinking water supplies. In South Dakota, attackers targeted a wastewater lift station in Rapid City; officials report no effect on drinking water quality or public safety. Georgia systems were also affected [4][5][6]. The FBI count of "at least seven states" indicates additional states have not been publicly identified [1][6].

The exposure problem, by the numbers. Forescout research found 4,407 devices worldwide exposing EtherNet/IP port 44818 to the internet, with about 65 percent located in the United States [5]. MicroLogix 1400 controllers make up 50 percent of those exposed assets; MicroLogix 1100 controllers make up 8 percent [5]. About 70 percent of the exposed U.S. controllers sit on large mobile carrier networks, connected through cellular routers, the same remote-connectivity pattern named in the federal alert [1][5].

Forescout also found 22 exposed hosts in the cities targeted in this campaign, and about 86 percent of them (19 of 22) were susceptible to CVE-2017-16740, a known denial-of-service vulnerability [5]. Older MicroLogix vulnerabilities (CVE-2016-5645, CVE-2017-7898 through CVE-2017-7903) also affect these device families [5].

Attribution. As of this release, neither the FBI nor state authorities have formally attributed the July campaign to a named actor [3][4]. Investigators have noted technical similarities to an Iranian-affiliated campaign documented in the joint CISA advisory AA26-097A (updated July 22, 2026), which describes actors using legitimate engineering software (Studio 5000 Logix Designer, EcoStruxure Control Expert, and Siemens TIA Portal) from leased third-party infrastructure to reach misconfigured controllers and exfiltrate PLC project files since at least March 2026 [4]. There is no confirmed link between the two campaigns [4][5].

Recommended Actions

Limehawk recommends that utilities and industrial operators apply the FBI and EPA guidance now:

- **Disconnect PLCs from the public-facing internet.** Broker all remote access through a secure gateway (jump host).
- **Secure cellular modems** with strong authentication and current firmware. Enable and review modem logs.
- **Set complex, unique passwords** on every OT device.
- **Restrict network access to PLCs** with firewall rules or access control lists. Allow only authorized control-system traffic. Block IP addresses associated with hosting providers, which the actors used as attack infrastructure.
- **Place physical and software key switches in the run position.** Validate project files before you switch modes.
- **Review project files and ladder logic** for unauthorized changes. Verify backups before you restore them.
- **Maintain and test the ability to run operations manually.**
- **Plan replacements for end-of-life hardware** that no longer receives security patches.

Organizations that experience similar OT outages should contact their local FBI field office and file a complaint at https://www.ic3.gov. CISA's 24/7 Operations Center is available at contact@cisa.dhs.gov or 1-844-729-2472. Include PLC model numbers, serials, and IP addresses, plus any unusual IPs seen on connected networks [2]. Water utilities can also request help through the EPA's Cybersecurity Technical Assistance Program for the Water Sector: https://www.epa.gov/cyberwater/forms/cybersecurity-technical-assistance-program-water-sector [2].

For deeper hardening guidance, the PSA points to four earlier federal documents: "Primary Mitigations to Reduce Cyber Threats to Operational Technology," the "Incident Response Guide: Water and Wastewater Sector," "Top Cyber Actions for Securing Water Systems," and "Secure Connectivity Principles for Operational Technology" [2].

About Limehawk

Limehawk, LLC is a managed IT services provider based in Knoxville, Tennessee. Limehawk designs, secures, and supports networks and IT operations for small businesses and organizations in East Tennessee, including secure remote access, firewall configuration, monitoring, and ongoing managed services. Learn more at https://limehawk.io.

Sources

1. FBI & EPA, “Malicious Cyber Actors Targeting Water and Wastewater Sector Internet-Facing Programmable Logic Controllers, Causing Operational Disruptions,” PSA, July 30, 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. IC3, Alert Number I-073026-PSA (PDF), July 30, 2026. https://www.ic3.gov/PSA/2026/PSA260730.pdf
3. Picus Security, “Minnesota Water Systems Attacks: Internet-Exposed PLCs Under Attack.” https://www.picussecurity.com/resource/blog/minnesota-water-systems-attacks-internet-exposed-plcs-under-attack
4. LevelBlue SpiderLabs, “Review of the July 2026 Cyberattacks Against U.S. Water and Wastewater Systems.” https://www.levelblue.com/blogs/spiderlabs-blog/review-of-the-july-2026-cyberattacks-against-u.s.-water-and-wastewater-systems
5. Forescout, “OT Security Analysis: Exposed Devices Attacked in US Water Systems.” https://www.forescout.com/blog/ot-security-analysis-exposed-devices-attacked-in-us-water-systems/
6. Newsweek, “Map Shows States Hit by Cyberattacks on Water Systems.” https://www.newsweek.com/map-shows-states-hit-by-cyberattacks-water-systems-12274817

Media Contact

Corey Watson, Managing Member
Limehawk, LLC
press@limehawk.io
https://limehawk.io

###