FEDERAL BUREAU OF INVESTIGATION
Public Service Announcement

Alert: I-073026-PSA | 30 JULY 2026

Malicious Cyber Actors Targeting Water and Wastewater Sector Internet-Facing Programmable Logic Controllers, Causing Operational Disruptions

INTRODUCTION

The Federal Bureau of Investigation (FBI) and Environmental Protection Agency (EPA) are issuing this Public Service Announcement (PSA) to warn critical infrastructure asset owners and operators that malicious cyber actors (MCAs) are conducting cyber attacks targeting Operational Technology (OT) devices, including Rockwell Automation/Allen-Bradley Programmable Logic Controllers (PLCs), specifically MicroLogix 1100 and 1400 series. Since 27 July 2026, Water and Wastewater Sector (WWS) utility companies in at least seven states have reported incidents to the FBI, and some of that activity degraded water operations. While the FBI has only observed this behavior with the referenced Rockwell PLCs, similar considerations should also be made with other branded PLCs.

After remotely accessing internet-facing devices, the actors changed the IP addresses and passwords, resulting in a loss of monitoring and control functionality. To reduce the risk of compromise, the FBI and EPA recommend **removing PLCs from direct internet exposure** via secure gateway and firewalls, setting up **strong, unique passwords**, and utilizing an **access control list (ACL)** to allow only authorized communication between expected control system devices.

THREAT LANDSCAPE

MCAs are targeting internet-exposed PLCs (Rockwell Automation/Allen-Bradley's MicroLogix 1100 and 1400 series) to remotely tamper with device configurations by changing IP addresses and turning on and setting passwords, resulting in a loss of view, and in some cases function, of connected equipment in targeted facilities. At least one organization reported modified PLC project files after noticing ladder logic discrepancies across several sites. Additionally, across several victims, similarities in network setup provided by third parties may provide MCA the opportunity to multiply successes when vulnerable network and hardware setups exist across customers.

Operational effects reported to the FBI have included loss of pressure and flooding. Pressure loss in water systems could potentially allow untreated ground water to seep into pipes. Once compromised, the extent of impact to victims' operations depended upon the type of function for which the PLC was configured (monitoring versus controlling equipment), the equipment itself (1100 versus 1400), the function the device supported, and capability to switch to manual operations. The FBI and EPA are engaging with victim organizations and are providing the following recommendations for critical infrastructure asset owners and operators.

Tips to Protect Yourself

The FBI and EPA recommend individuals take the following precautions:

- **Disconnect PLC from the public-facing internet.** Follow the joint guidance Secure connectivity principles for OT to safely allow remote access. Specifically, "remove inbound port exposure," so the OT system is never directly exposed to the internet or external networks, and to ensure all access is mediated, monitored, and controlled. Do this through a secure gateway (jump host) that brokers the connection.
    - Ensure cellular modems, used for remote field connectivity and access, are secured with strong authentication and updated.
    - Enable logs for connected modems and regularly review for suspicious activity to detect intrusions and improve incident response speed.
    - To mitigate unauthorized access to OT via cellular modems, organizations should consider implementing isolated architectures, such as private Access Point Name (APN), 5G Public Network Integrated Non-Public Network (PNI-NPN), cellular Software-Defined Wide Area Network (SD-WAN), Zero Trust Network Access (ZTNA), or a site-to-site virtual private network (VPN).

- **Ensure device passwords are complex, unique combinations of letters, numbers, and symbols** that are not easily guessable. Implementing robust password practices remains a critical security measure that can help prevent unauthorized access and strengthen the overall security posture of OT devices.

- **Strictly control network access to PLC devices.** Configure firewall rules or access control list (ACL) security features on PLCs or programmable controllers to allow only authorized communications between expected control system devices. Block access from unauthorized or threat actor-controlled IP addresses, such as those associated with hosting providers

- **Place physical and software key switches into the run position** to block unauthorized changes to logic, configuration, and firmware. Devices should only be in the program or remote position when updating or downloading software online and immediately switched back to the run position when complete. (See Rockwell Automation's System Security Design Guidelines for manufacturer's instructions.)

  - Prior to switching the device to run mode, review and validate project files, as changing modes will lock in the current project file downloaded to the device.

- **Practice and maintain the ability to operate OT systems manually.** The capability for organizations to revert to manual controls to quickly restore operations is vital in the immediate aftermath of an incident. Business continuity and disaster recovery plans, fail-safe mechanisms, islanding capabilities, software backups, and standby systems should all be routinely tested to ensure safe manual operations in the event of an incident.

- **Review project files running on PLCs for unauthorized changes.** Use vendor provided integrity checking tools and visually compare the running program to known good logic. Ensure reusable logic and input/output configurations are valid.
  - If restoring backups, verify the backup does not contain malicious logic before deployment.
  - Review logs and configurations on all connected devices, including modems, HMIs, and workstations, to assess potential lateral movement by threat actors. If it appears the actors connected to additional devices, reimage these devices to remove any potential malicious changes or access tools.

- **Plan for end-of-life (EOL) replacements** when possible. When a hardware device is EOL, the manufacturer no longer sells the product and is not actively supporting the hardware, which also means they are no longer releasing software updates or security patches for the device. Since EOL devices no longer receive security updates, they are routinely targeted by MCAs.
  - Maintain a rolling 12-month EOL forecast, reviewed quarterly with owners and procurement.
  - Track EOL systems by product, owner, location, and retirement date.
  - Replace or isolate EOL assets; if delays occur, apply compensating controls with firm decommission dates.

REPORT IT

If you or someone you know has sustained similar OT outages, please contact your local FBI Field Office and file a complaint with the IC3 at www.ic3.gov. Additionally, you can contact CISA via CISA's 24/7 Operations Center at contact@cisa.dhs.gov or 1-844-Say-CISA (1-844-729-2472). Be sure to include as much information as possible:

- Model numbers, serials, and IPs of programmable logic controllers connected to network
- Unusual IPs on networks connected to programmable logic controllers

EPA's Cybersecurity Technical Assistance: https://www.epa.gov/cyberwater/forms/cybersecurity-technical-assistance-program-water-sector

Rockwell Automation: Contact the Rockwell Automation Product Security Incident Response Team (PSIRT) at PSIRT@rockwellautomation.com for questions regarding this guidance, or to report cyber incidents related to Rockwell Automation products.

For additional information on mitigating threats to OT systems, please see previous Guidance Documents:

- FBI, CISA, EPA, DOE | Primary Mitigations to Reduce Cyber Threats to Operational Technology
- FBI, CISA, EPA | Incident Response Guide: Water and Wastewater Sector
- FBI, CISA, EPA | Top Cyber Actions for Securing Water Systems
- NCSC-UK, FBI, CISA | Secure connectivity principles for operational technology (OT)

Disclaimer: The information in this document is being provided "as is" for informational purposes only. The FBI does not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by FBI.