*Co-Authored by:*



# Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure

**Publication: April 7, 2026**

**Federal Bureau of Investigation**
**Cybersecurity and Infrastructure Security Agency**
**National Security Agency**
**Environmental Protection Agency**
**Department of Energy**
**United States Cyber Command – Cyber National Mission Force**

*To report suspicious or criminal activity related to information found in this joint Cybersecurity Advisory, contact your local FBI field office or CISA's 24/7 Operations Center at contact@cisa.dhs.gov or 1-844-Say-CISA (1-844-729-2472). When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. For NSA-client requirements or cybersecurity inquiries, contact Cybersecurity_Requests@nsa.gov.*

## Advisory at a Glance

| | |
|---|---|
| **Title** | Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure |
| **Original Publication** | April 7, 2026 |
| **Executive Summary** | Iran-affiliated advanced persistent threat (APT) actors are conducting exploitation activity targeting internet-facing operational technology (OT) devices, including programmable logic controllers (PLCs) manufactured by Rockwell Automation/Allen-Bradley. This activity has led to PLC disruptions across several U.S. critical infrastructure sectors through malicious interactions with the project file and manipulation of data on human machine interface (HMI) and supervisory control and data acquisition (SCADA) displays, resulting in operational disruption and financial loss.<br><br>U.S. organizations should urgently review the tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) in this advisory for indications of current or historical activity on their networks, and apply the recommendations listed in the **Mitigations** section of this advisory to reduce the risk of compromise. |
| **Affected Products** | ▪ Rockwell Automation/Allen-Bradley manufactured PLCs<br>▪ Potentially other branded PLCs |
| **Key Actions** | ▪ Remove PLCs from direct internet exposure via secure gateway and firewall.<br>▪ Query available logs for the provided IOCs in the corresponding time frames.<br>▪ Check available logs for suspicious traffic on the ports associated with OT devices, including `44818`, `2222`, `102`, and `502`, especially traffic originating from overseas hosting providers.<br>▪ For Rockwell Automation devices, place the physical mode switch on the controller into run position. Contact the authoring agencies and Rockwell Automation for guidance if you believe your organization was targeted. |
| **Indicators of Compromise** | For a downloadable copy of IOCs, see:<br>▪ AA26-097A STIX XML (15 KB)<br>▪ AA26-097A STIX JSON (14 KB) |
| **Intended Audience** | **Organizations:** Critical Infrastructure<br><br>**Sectors:** Government Services and Facilities, Water and Wastewater Systems (WWS), and Energy<br><br>**Roles:** Defensive cybersecurity analysts, OT cybersecurity engineers, cybersecurity architects, secure systems developer |

# Table of Contents

## Introduction

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Environmental Protection Agency (EPA), Department of Energy (DOE), and United States Cyber Command – Cyber National Mission Force (CNMF), hereafter referred to as the "authoring agencies," are urgently warning U.S. organizations of ongoing cyber exploitation of internet-connected operational technology (OT) devices, including Rockwell Automation/Allen-Bradley-manufactured programmable logic controllers (PLCs), across multiple U.S. critical infrastructure sectors. As a result of this activity, organizations from multiple U.S. critical infrastructure sectors experienced disruptions through malicious interactions with the project files[1] and the manipulation of data displayed on human machine interface (HMI) and supervisory control and data acquisition (SCADA) displays. In a few cases, this activity has resulted in operational disruption and financial loss.

Due to the widespread use of these PLCs and the potential for additional targeting of other branded OT devices across critical infrastructure, the authoring agencies recommend U.S. organizations urgently review the tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) in this advisory for indications of current or historical activity on their networks, and apply the recommendations listed in the **Mitigations** section to reduce the risk of compromise.

The authoring agencies assess a group of Iranian-affiliated advanced persistent threat (APT) actors is conducting this activity to cause disruptive effects within the United States. The group has targeted devices spanning multiple U.S. critical infrastructure sectors, including Government Services and Facilities (to include local municipalities), Water and Wastewater Systems (WWS), and Energy Sectors. The authoring agencies previously reported on similar activity targeting PLCs by CyberAv3ngers (aka Shahid Kaveh Group)—a cyber threat actor affiliated with Iran's Islamic Revolutionary Guard Corps (IRGC) Cyber Electronic Command (CEC).

If owners and operators discover an affected internet-accessible device in their environment, additional technical measures may be necessary to evaluate the risk of compromise. Please contact the authoring agencies and applicable vendors through existing support channels available to customers and integrators (see **Contact Information**) to receive support, mitigation, and investigation assistance, and engage your cyber incident response plans.

In addition to contacting the authoring agencies, organizations with Rockwell Automation/Allen-Bradley-manufactured PLCs should review the manufacturer's previously issued guidance to strengthen the security of their operational technology deployments: PN1550 | CVE-2021-22681: Authentication Bypass Vulnerability Found in Logix Controllers, published in 2021, and SD1771 | Rockwell Automation Reiterates Customer Guidance to Disconnect Devices from the Internet and Harden PLCs to Protect from Cyber Threats, published in 2026. 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 more information on Iranian malicious cyber activity, see CISA's Iran Threat Overview and Advisories webpage and the FBI's Iran Threat webpage.

For a downloadable copy of IOCs, see:

- AA26-097A STIX XML (15 KB)
- AA26-097A STIX JSON (14 KB)

# Background Information

## Similar Historical Activity Targeting Programmable Logic Controllers

During a similar campaign beginning in November 2023, the IRGC CEC-affiliated cyber threat actors known as "CyberAv3ngers" targeted U.S.-based PLCs and HMIs, causing disruptive effects. Private industry and open sources also refer to this group as Hydro Kitten, Storm-0784, APT Iran, Bauxite, Mr. Soul, Soldiers of Solomon, UNC5691, and the Shahid Kaveh Group. These attacks compromised at least 75 devices, targeting U.S.-based Unitronics PLC devices with an HMI used across multiple critical infrastructure sectors, including WWS. For more information on this group's activity, see the authoring agencies' Joint Cybersecurity Advisory IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities.

## Ongoing Threat Actor Activity Against U.S.-Based Programmable Logic Controllers

The FBI assesses a group of Iranian-affiliated APT actors are targeting internet-exposed PLCs with the intent to cause disruptions—including maliciously interacting with project files, and manipulating data displayed on HMI and SCADA displays—to U.S. critical infrastructure organizations. Iranian-affiliated APT targeting campaigns against U.S. organizations have recently escalated, likely in response to hostilities between Iran, and the United States and Israel.

Since at least March 2026, the authoring agencies identified (through engagements with victim organizations) an Iranian-affiliated APT-group that disrupted the function of PLCs. These PLCs were deployed across multiple U.S. critical infrastructure sectors (including Government Services and Facilities, WWS, and Energy sectors) within a wide variety of industrial automation processes. Some of the victims experienced operational disruption and financial loss.

# Technical Details

**Note:** This advisory uses the MITRE ATT&CK® Matrix for Enterprise framework, version 18. See the **MITRE ATT&CK Tactics and Techniques** section of this advisory for tables of the threat actors' activity mapped to MITRE ATT&CK tactics and techniques.

## Initial Access

The authoring agencies observed Iranian-affiliated APT actors using several overseas-based IP addresses to access internet-facing Rockwell Automation/Allen-Bradley-manufactured PLCs [T0883]. The actors used leased, third-party hosted infrastructure with configuration software, such as Rockwell Automation's Studio 5000 Logix Designer software, to create an accepted connection to the victim's PLC. Targeted devices include CompactLogix and Micro850 PLC devices.

## Command and Control

Inbound malicious traffic may be directed to devices on any of following ports: `44818`, `2222`, `102`, `22`, or `502`. The targeting of ports [T0885] associated with other OT vendors' protocols suggests these actors may also be targeting devices manufactured by companies other than Rockwell Automation/Allen-Bradley,

including the Siemens S7 PLC. Additionally, the actors deployed Dropbear Secure Shell (SSH) software on victim endpoints to enable them to gain remote access through port 22 [T1219].

### Impact

The FBI identified that this activity resulted in the extraction of the device's project file and data manipulation on HMI and SCADA displays [T1565].

## Indicators of Compromise

See **Table 1** for recent IP addresses used by the Iranian-affiliated APT actors to communicate with Rockwell Automation/Allen-Bradley-manufactured devices (and potentially other branded OT devices) in the United States.

**Disclaimer:** The FBI observed that the threat actors used the IP addresses listed below in the specified time frames. This data is being provided for customers to query against logs for indications of historical targeting by the Iranian-affiliated APT actors. The authoring agencies recommend organizations investigate or vet these IP addresses prior to taking action, such as blocking.

*Table 1. Indicators of Compromise*

| Indicator | Beginning of Actor Association | End of Actor Association |
|---|---|---|
| 135.136.1[.]133 | March 2026 | March 2026 |
| 185.82.73[.]162 | January 2025 | March 2026 |
| 185.82.73[.]164 | January 2025 | March 2026 |
| 185.82.73[.]165 | January 2025 | March 2026 |
| 185.82.73[.]167 | January 2025 | March 2026 |
| 185.82.73[.]168 | January 2025 | March 2026 |
| 185.82.73[.]170 | January 2025 | March 2026 |
| 185.82.73[.]171 | January 2025 | March 2026 |

## MITRE ATT&CK Tactics and Techniques

See **Table 2** to **Table 4** for all referenced threat actor tactics and techniques in this advisory. The authoring agencies recommend organizations review historical TTPs for similar Iranian-affiliated cyber actor activity in IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities. For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, see CISA and MITRE ATT&CK's Best Practices for MITRE ATT&CK Mapping and CISA's Decider Tool.

*Table 2. Initial Access*

| Technique Title | ID | Use |
|---|---|---|
| Internet Accessible Device | T0883 | The actors used Rockwell Automation's programming software (such as Studio 5000 Logix Designer) to access and interact with publicly exposed, internet-accessible PLCs installed and deployed without sufficient network and/or hardening security controls. |

*Table 3. Impact*

| Technique Title | ID | Use |
|---|---|---|
| Stored Data Manipulation | T1565 | The actors maliciously interacted with project files and altered data displayed on HMI and SCADA displays. |

*Table 4. Command and Control*

| Technique Title | ID | Use |
|---|---|---|
| Commonly Used Port | T0885 | The actors used commonly used OT ports to communicate with PLCs. |
| Remote Access Tools | T1219 | The actors deployed Dropbear SSH software on victim endpoints to enable them to gain remote access through port 22. |

## Mitigations

The authoring agencies recommend organizations implement the mitigations below to improve your organization's cybersecurity posture on the basis of the threat actors' activity. These mitigations align with the Cross-Sector Cybersecurity Performance Goals 2.0 (CPGs 2.0) developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats, tactics, techniques, and procedures. Visit CISA's CPG 2.0 webpage for more information on the CPGs, including additional recommended baseline protections.

### Network Defenders

The cyber threat actors accessed Rockwell Automation/Allen-Bradley-manufactured PLCs to cause disruptions to victim systems. To safeguard against this threat and threats to other types of PLCs, the authoring agencies urge organizations to consider the following mitigations.

In addition, organizations with these PLCs should view Rockwell Automation's guidance: Rockwell Automation Reiterates Customer Guidance to Disconnect Devices from the Internet and Harden PLCs to Protect from Cyber Threats.

**Immediate steps to prevent the attack:**

- **Disconnect the PLC from the public-facing internet** [CPG 3.S]. 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 the connected modems to detect intrusion and improve incident response speed.
- **For controllers with a physical mode switch, place the physical mode switch into run position to prevent remote modification.** 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's[2] System Security Design Guidelines for manufacturer's instructions.)
- **For devices that allow for software key switching,** enable programming protection in PLC configuration software (S7 Totally Integrated Automation [TIA] Portal) to limit who can modify PLCs remotely. (See Siemens' Cybersecurity for Industry Operational Guidelines for the manufacturer's instructions.)
- **Create and test strong backups of the logic and configurations of PLCs**. Store backup files offline and secure the physical removal media to enable fast recovery.

**Follow-up steps to strengthen security posture:**

- **Implement multifactor authentication (MFA)** [CPG 3.F] for access to the OT network from an external network.
- If remote access is required, **implement a network proxy, gateway, firewall, and/or virtual private network (VPN) in front of the PLC to control network access**.
  - A VPN or gateway device can enable MFA for remote access even if the PLC does not support MFA. Implement security rules on these higher-level network security mechanisms that prevent the type of repeated and sustained login attempts that would be seen during a brute force attack. When possible, implement a device control list for workstations sending messages or connecting to OT components.
  - Use the device control list to monitor for logon activity for unexpected or unusual access to devices from the internet.
- **Keep PLC devices updated with the latest software patches by the manufacturer.** Use established downtime windows to install patches. Known Exploited Vulnerabilities may need to be prioritized outside a downtime window.
- **Configure external and internal firewalls to block traffic using common ports** associated with network protocols that are unnecessary for the particular network segment.

- **Disable any unused authentication methods, logic, or features,** such as default authentication keys, as well as unused or needed services such as Teletype Network (Telnet), File Transfer Protocol (FTP), Remote Desktop Protocol (RDP), Virtual Network Computing (VNC), and web services.
- **Monitor asset management systems for device configuration changes**, which can be used to understand expected parameter settings.
- **Monitor the content of network traffic** for the following:
  - Unusual logins to internet-connected devices or unexpected protocols to/from the internet.
  - Functions of industrial control systems (ICS) management protocols that change an asset's operating mode or modify programs.

In addition, the authoring agencies recommend network defenders apply the following mitigations to limit potential adversarial use of common system and network discovery techniques, as well as reduce the impact and risk of compromise by cyber threat actors:

- **Reduce risk exposure.** CISA offers a range of services at no cost, including scanning and testing, to help organizations reduce exposure to threats via mitigating attack vectors. CISA's Cyber Hygiene Services can help provide additional review of organizations' internet accessible assets.

## Device Manufacturers

**Note:** The following guidance is general in nature and not specific to any OT vendor. Some of the features, settings, and practices may already be offered by certain vendors. The inclusion of this guidance should not be interpreted as an assertion that vendors referenced in this product do not offer such security features.

Although critical infrastructure organizations using PLC devices can take steps to mitigate the risks, it is ultimately the responsibility of the device manufacturer to build products that are secure by design and default. The authoring agencies urge device manufacturers to take ownership of their customers' security outcomes by following the principles in the joint guide Secure by Demand: Priority Considerations for OT Owners and Operators when Selecting Digital Products, primarily:

- Change the manufacturers' default settings to prevent exposing administrative interfaces to the internet.
- Do not charge additional fees for basic security features needed to operate the product securely.
- Support MFA, including via phishing-resistant methods.

By using secure by design tactics, software manufacturers can make product lines secure "out of the box" without requiring customers to spend additional resources making configuration changes, purchasing tiered security software and logs, monitoring, and making routine updates.

For more information on common misconfigurations and guidance on reducing their prevalence, see joint advisory NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations. For more information on secure by design, see CISA's Secure by Design webpage and joint guide.

## Validate Security Controls

In addition to applying mitigations, the authoring agencies recommend exercising, testing, and validating your organization's security program against the threat behaviors mapped to the MITRE ATT&CK for Enterprise framework in this advisory. The authoring agencies recommend testing your existing security controls inventory to assess how they perform against the ATT&CK techniques described in this advisory.

To get started:

1. Select an ATT&CK technique described in this advisory (see **Table 2** to **Table 4**).
2. Align your security technologies against the technique.
3. Test your technologies against the technique.
4. Analyze your detection and prevention technologies' performance.
5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program, including people, processes, and technologies, based on the data generated by this process.

The authoring agencies recommend continually testing your security program, at scale, in a production environment to ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

## Resources

- Authoring Agencies: IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities
- CISA: Bulletproof Defense: Mitigating Risks From Bulletproof Hosting Providers
- EPA: Cybersecurity for the Water Sector
- CISA: Water and Wastewater Systems Sector
- CISA Alert: Exploitation of Unitronics PLCs used in Water and Wastewater Systems
- CISA: Iran Threat Overview and Advisories
- FBI: The Iran Threat
- CISA, MITRE: Best Practices for MITRE ATT&CK Mapping
- CISA: Decider Tool
- CISA: Cross-Sector Cybersecurity Performance Goals 2.0
- CISA: No-Cost Cybersecurity Services and Tools
- CISA: Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products
- NSA, CISA: NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations
- CISA: Secure by Design
- FBI: Primary Mitigations to Reduce Cyber Threats to Operational Technology

- United Kingdom National Cyber Security Center: Secure connectivity principles for operational technology (OT)

## Contact Information

U.S. organizations are encouraged to report suspicious or criminal activity related to information in this advisory to CISA, FBI, and/or NSA:

- Contact CISA via CISA's 24/7 Operations Center at contact@cisa.dhs.gov or 1-844-Say-CISA (1-844-729-2472) or your local FBI field office. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.
- For NSA cybersecurity guidance inquiries, contact CybersecurityReports@nsa.gov.
- Entities required to report incidents to DOE should follow established reporting requirements, as appropriate. For other energy sector inquiries, contact EnergySRMA@hq.doe.gov.
- Contact the Rockwell Automation PSIRT for questions regarding their guidance or for reporting cyber incidents related to Rockwell Automation at PSIRT@rockwellautomation.com.

## Disclaimer

The information in this report is being provided "as is" for informational purposes only. The authoring agencies do 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 the authoring agencies.

## Version History

**April 7, 2026**: Initial version.

## Notes

[1] Project file refers to the software file that contains ladder logic and configuration settings. On Rockwell Automation devices, it is referred to as an .ACD file.

[2] See CompactLogix 5370 Controllers (Chapter 5: "Select the Operating Mode of the Controller") for more information on functions available for the switch.