JOINT
CYBERSECURITY ADVISORY

TLP:CLEAR

Product ID: AA26-097A

Co-Authored by:

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

Publication: April 7, 2026

Last Update: July 22, 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
Department of the Treasury

To report suspicious or criminal activity related to information found in this joint Cybersecurity Advisory, contact the FBI's Internet Crime Complaint Center (IC3), your local FBI field office, and/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
Last Update	July 22, 2026
Executive Summary	The authoring agencies urgently warn U.S. organizations of ongoing Iranian-affiliated cyber targeting of internet-connected operational technology (OT) devices, including programmable logic controllers (PLCs). These actions disrupted PLCs across several U.S. critical infrastructure sectors through malicious project file interactions and manipulation of data on human machine interface (HMI) and supervisory control and data acquisition (SCADA) displays, resulting in operational disruption and financial loss.
Last Update Description	This update adds new guidance on detecting malicious changes in reusable code modules exploited within Rockwell Automation PLC programs. It also expands scope to include observed targeting of Schneider Electric, Siemens, and potentially other branded/manufactured PLCs, emphasizing the importance of restricting direct internet access and providing best practices for secure deployment.
Affected Products	Potentially all internet exposed PLCs, including Rockwell Automation/Allen-Bradley, Schneider Electric, Siemens, and other branded/manufactured PLCs.
Key Actions	▪ Install PLCs consistent with manufacturers' guidelines and security best practices. ▪ Remove PLCs from direct internet exposure via secure gateway and firewall; work with IT/OT team members and/or integrators to perform this action. ▪ Query available logs for the provided indicators of compromise (IOCs) and check available logs for suspicious traffic on the ports associated with OT devices, including `44818`, `2222`, `102`, and `502`, especially traffic originating from foreign hosting providers. ▪ For Rockwell Automation devices, place the physical mode switch on the controller into run position. If you suspect your organization was targeted, including against other branded PLC devices, contact the authoring agencies and PLC manufacturer for guidance.
Indicators of Compromise	For a downloadable copy of July 22, 2026 IOCs, see: ▪ AA26-097A STIX XML (July 2026) (29 KB) ▪ AA26-097A STIX JSON (July 2026) (30 KB) For a downloadable copy of historical April 7, 2026 IOCs, see: ▪ AA26-097A STIX XML (36 KB) ▪ AA26-097A STIX JSON (12 KB)
Intended Audience	**Organizations:** Critical Infrastructure **Sectors:** Government Services and Facilities, Water and Wastewater Systems (WWS), and Energy **Roles:** Integrators, asset owners, defensive cybersecurity analysts, OT cybersecurity engineers, cybersecurity architects, secure systems developer

Table of Contents

Introduction

Note: *This advisory was originally published on April 7, 2026, to provide tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) related to ongoing cyber exploitation of internet-connected operational technology (OT) devices by Iranian-affiliated advanced persistent threat (APT) actors. The authoring agencies updated this advisory on July 22, 2026, to add new guidance on detecting malicious changes in reusable code modules leveraged within Rockwell Automation PLC programs. It also expands the manufacturer scope to include observed targeting of Schneider Electric, Siemens, and potentially other branded/manufactured PLCs, emphasizing the importance of restricting direct internet access and providing best practice resources for secure deployment.*

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Environmental Protection Agency (EPA), Department of Energy (DOE), United States Cyber Command – Cyber National Mission Force (CNMF), and Department of the Treasury (Treasury) (hereafter referred to as the "authoring agencies") are urgently warning U.S. organizations of ongoing cyber exploitation of internet-connected OT devices—including PLCs manufactured by Rockwell Automation/Allen-Bradley, Schneider Electric, Siemens, and potentially other manufactured 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 PLC 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 caused operational disruption and financial loss.

The authoring agencies assess a group of Iranian-affiliated APT actors is conducting this activity to cause disruptive effects within the United States. The group 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).

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 TTPs and 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.

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 engage your cyber incident response plans and 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.

For more information on Iranian malicious cyber activity, see CISA's Iran Threat Overview and Advisories webpage and the FBI's Iran Threat and Iran Cyber Threat Overview webpages.

(New, July 22, 2026) For a downloadable copy of July 22, 2026 IOCs, see:

- AA26-097A STIX XML (29 KB)
- AA26-097A STIX JSON (30 KB)

For a downloadable copy of historical April 7, 2026 IOCs, see:

- AA26-097A STIX XML (36 KB)
- AA26-097A STIX JSON (12 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 the WWS. APT actors developed and deployed custom ladder logic code to these devices, replacing the valid ladder logic with malicious code that continues to be observed to date.

For more information on this group's activity, see the 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 observed Iranian-affiliated APT actors 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. critical infrastructure have recently escalated, likely in response to hostilities between Iran, and the United States and Israel.

(New, July 22, 2026) At one U.S. victim, the FBI observed the APT actors download a malicious project file to a targeted PLC using configuration software. Analysis indicated the project file retained ladder logic for downstream function but added logic that overrode specific instruction sets responsible for maintaining safe operating parameters in the victim's environment.

Since at least March 2026, the authoring agencies identified (through engagements with victim organizations) an Iranian-affiliated APT group disrupted the function of PLCs. Organizations across several U.S. critical infrastructure sectors (including Government Services and Facilities, WWS, and Energy Sectors) deployed these PLCs 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 19. 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

(Updated, July 22, 2026) The authoring agencies observed Iranian-affiliated APT actors using several foreign-based IP addresses to access internet-facing PLCs manufactured by Rockwell Automation/Allen-Bradley, Schneider Electric, Siemens, and potentially other manufactured PLCs [T0883]. The actors used leased, third-party hosted infrastructure and manufacturers' PLC programming software to connect to misconfigured victim PLCs. Inbound malicious traffic has been observed targeting PLC devices on the following ports: `44818`, `2222`, `102`, and `502`, as well as targeting modems on port `22`. Targeted devices include:

- **Rockwell Automation:** CompactLogix and Micro850 PLCs
- **Schneider Electric:** BMX P34/Modicon M340 PLCs
- **Siemens:** S7-1200 series PLCs

Command and Control

(Updated, July 22, 2026) The targeting of ports [T0885] associated with other OT vendors' protocols suggests these actors are opportunistically targeting devices manufactured by companies other than Rockwell Automation/Allen-Bradley, including Schneider Electric and Siemens. In one reported instance, the actors utilized Dropbear Secure Shell (SSH) software on victim modems to enable them to gain remote access through port `22` [T1219].

Exfiltration

(New, July 22, 2026) The authoring agencies observed Iranian-affiliated APT actors using configuration software—such as Rockwell Automation's Studio 5000 Logix Designer, Schneider Electric's EcoStruxure Control Expert, and Siemens' Totally Integrated Automation (TIA) Portal—on leased, third-party hosted infrastructure to exfiltrate device project files from PLC devices to threat-actor-controlled infrastructure [T1041].

Impact

(Updated, July 22, 2026) After the actors extracted device project files, the FBI and CISA identified the modification and deletion of project file logic, to include Add-On Instructions (AOIs) and data manipulation on HMI and SCADA displays [T1565]. Additionally, the changes disabled critical shutdown and alarm logic, allowing systems to enter unsafe conditions without notifying operators of the anomalies.

Note: An AOI is analogous to a "Function Block" or "User Defined Function Block" used in other PLC vendor programs.

Indicators of Compromise

See **Table 1** and **Table 2** for recent IP addresses used by the Iranian-affiliated APT actors to communicate with PLCs manufactured by Rockwell Automation/Allen-Bradley, Schneider Electric, and Siemens in the United States.

Disclaimer: The FBI observed the threat actors using 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 (New, July 22, 2026)

Indicator	Beginning of Actor Association	End of Actor Association
185.82.73[.]175	September 2025	February 2026
141.11.164[.]153	January 2026	July 2026
175.110.121[.]42	February 2026	March 2026
175.110.121[.]39	February 2026	March 2026
175.110.121[.]41	February 2026	March 2026
175.110.121[.]107	February 2026	February 2026
192.142.54[.]79	May 2026	June 2026
84.200.205[.]165	May 2026	June 2026
185.225.17[.]225	June 2026	July 2026
79.133.46[.]209	July 2026	July 2026
88.80.150[.]199	July 2026	July 2026
88.80.150[.]200	July 2026	July 2026
88.80.150[.]202	July 2026	July 2026

Table 2. Indicators of Compromise

Indicator	Beginning of Actor Association	End of Actor Association
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
135.136.1[.]133	March 2026	March 2026

MITRE ATT&CK Tactics and Techniques

See **Table 3** to **Table 6** 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 3. Initial Access

Technique Title	ID	Use
Internet Accessible Device	T0883	The actors accessed and interacted with publicly exposed, internet-accessible PLCs that lacked sufficient network and/or hardening security controls.

Table 4. Command and Control

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

Table 5. Exfiltration (New, July 22, 2026)

Technique Title	ID	Use
Exfiltration Over C2 Channel	T1041	The actors used remote, third-party hosted infrastructure as a C2 channel to transfer device project files out of victim environments.

Table 6. Impact

Technique Title	ID	Use
Data Manipulation	T1565	The actors maliciously interacted with project files, including modifying and deleting project file logic, and altered data displayed on HMI and SCADA displays.

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 (CPGs) 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 and TTPs. Visit CISA's CPGs webpage for more information on the CPGs, including additional recommended baseline protections.

Network Defenders

The cyber threat actors accessed PLCs manufactured by Rockwell Automation/Allen-Bradley, Schneider Electric, Siemens, and potentially other branded/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.

(Updated, July 22, 2026) In addition to contacting the authoring agencies, organizations and integrators operating PLCs from the manufacturers mentioned in this advisory should review the previously issued guidance to strengthen the security of their OT deployments:

- **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.
  - Refer to Rockwell Automation Security Advisory SD1771 for recommended PLC hardening measures and configuration guidance.
- **Schneider Electric:** Contact the Schneider Electric Corporate Product Cyber Emergency Response Team (CPCERT) at cpcert@se.com for questions regarding this guidance, or to report cyber incidents related to Schneider Electric products.

- Refer to Schneider Electric's Recommended Cybersecurity Best Practices and Cybersecurity User Guide for Modicon Controller Platform for guidance on securing and configuring PLCs.

- **Siemens:** Contact Siemens ProductCERT at productcert@siemens.com for questions regarding this guidance, or to report cyber incidents and vulnerabilities related to Siemens products.
  - Refer to Siemens Security Bulletin 104599 for a list of security measures to harden PLCs and in-depth configuration guides.
  - Siemens users should review the Cybersecurity for Industry Operational Guidelines and implement defense-in-depth controls within their automation systems.

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 connected modems and regularly review for suspicious activity to detect intrusions and improve incident response speed.
  - *(New, July 22, 2026)* 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).
- *(New, July 22, 2026)* **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.
- **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 Automation's[2] System Security Design Guidelines for manufacturer's instructions.)
  - *(New, July 22, 2026)* 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.
- **For devices that allow software key switching,** enable programming protection in PLC configuration software (S7 TIA Portal) to limit who can modify PLCs remotely. (See Siemens' Cybersecurity for Industry Operational Guidelines for the manufacturer's instructions.)

Follow-up steps to strengthen security posture:

- ***(New, July 22, 2026)*** **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. For Rockwell Automation PLCs listed in the Customer Guidance to Disconnect Devices from the Internet, check the AOIs for any anomalous modifications.
  - If restoring from 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.
- ***(New, July 22, 2026)*** **Ensure device passwords are changed from their default** and are configured to use 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.
- ***(New, July 22, 2026)*** **Take defensive measures to minimize the risk of exploitation.** Conduct comprehensive impact analysis and risk assessments prior to deploying defensive measures.
- **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.
- **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 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 to prevent the type of repeated and sustained login attempts 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 issued 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 and passwords, 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 management protocols that change an asset's operating mode or modify programs.
- ***(New, July 22, 2026)*** **Ensure service providers are informed of active threats targeting internet-connected PLC devices.** Owners and operators should communicate directly with service providers to address risks, especially when remote monitoring or maintenance is involved. Some service providers may rely on internet connectivity essential to monitor and maintain OT/ICS operations but may not be fully aware of active threats.

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 do not offer such security features. Also, this advisory is not highlighting a new vulnerability in the identified products, but instead discusses opportunistic targeting. Device manufacturers can make opportunistic attacks more difficult at scale by encouraging more secure behavior by default and in operations, as discussed below.

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 secured 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 3** to **Table 6**).
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 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 Cybersecurity
- CISA: Exploitation of Unitronics PLCs used in Water and Wastewater Systems
- CISA: Iran Threat Overview and Advisories
- FBI: The Iran Threat and Cyber Threat Overview: Iran
- 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 OT 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, CISA: Primary Mitigations to Reduce Cyber Threats to Operational Technology
- United Kingdom National Cyber Security Centre: Secure connectivity principles for operational technology

Contact Information

U.S. organizations are encouraged to report suspicious or criminal activity related to information in this advisory to CISA, the 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). File a claim with FBI's Internet Crime Complaint Center (IC3) or contact 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; and
  - 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 products at PSIRT@rockwellautomation.com.
- Contact the Schneider Electric CPCERT at cpcert@se.com for questions regarding this guidance, or to report cyber incidents related to Schneider Electric products.
- Contact Siemens ProductCERT for up-to-date information about the security of Siemens products or to report cybersecurity vulnerabilities at productcert@siemens.com. For support with increasing the security of installed Siemens PLCs, contact Siemens Industrial Cybersecurity Services at services.automation@siemens.com. See Siemens ProductCERT and Siemens CERT for more information.

Disclaimer

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

Version History

April 7, 2026: Initial version.

July 22, 2026: Update includes new guidance on detecting malicious activity, expanded scope of observed targeting, and best practices for secure PLCs deployment.

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.