INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-13 16:28 UTC

Iranian-Affiliated Cyber Actors Actively Targeting Rockwell Automation PLCs in US Critical Infrastructure

THREAT CAMPAIGN | **CRITICAL** | CVSS 9.1

SCC Item ID	SCC-CAM-2026-0172
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.1
Affected Products	Rockwell Automation and Allen-Bradley PLCs (specific models and firmware versions not confirmed from verified sources; Censys research indicates approximately 4,000 US-exposed industrial devices)
Published	2026-04-11
Discovery Source	Gemini

Executive Summary

Iranian state-affiliated cyber actors are actively targeting Rockwell Automation and Allen-Bradley programmable logic controllers (PLCs) deployed in US critical infrastructure, including power grid and water/wastewater systems. CISA advisory AA26-097A documents the campaign, which exploits internet-exposed industrial control systems with weak or default credentials to disrupt operations and manipulate physical processes. Organizations operating OT/ICS environments with internet-facing Rockwell Automation equipment face immediate operational disruption risk and potential physical consequences to industrial processes.

Technical Analysis

Iranian-affiliated threat actors are targeting Rockwell Automation and Allen-Bradley PLCs exposed directly to the internet, exploiting missing authentication controls and weak credential configurations to gain access to HMI/SCADA interfaces and manipulate industrial processes. Censys research identified approximately 4,000 US-based industrial devices in this exposure class. Attack methods align with MITRE ATT&CK for ICS techniques: valid account abuse (T1078), brute-force credential attacks (T1110), unauthorized command execution to PLCs (T0855), manipulation of control logic (T0816), internet-accessible device discovery (T0883), exploitation of external remote services (T1133), and manipulation of physical control processes (T0831). Relevant CWEs include CWE-306 (missing authentication for critical function), CWE-284 (improper access

control), CWE-1188 (insecure default initialization), and CWE-200 (information exposure). No specific CVEs have been confirmed in available source references as of this report. Specific affected firmware versions and model numbers have not been confirmed from verified sources. Refer to CISA AA26-097A and Rockwell Automation security advisories for vendor-confirmed affected configurations. CVSS base score assessed at 9.1 (Critical) for reference; no specific CVE match identified. EPSS data not available for this campaign-class item.

Action Checklist

1. Containment: Immediately audit all Rockwell Automation and Allen-Bradley PLCs for direct internet exposure. Remove any device from internet-facing network segments or place behind firewall/VPN with deny-all inbound rules. Reference CISA AA26-097A for scope guidance. If isolation is not immediately possible, block all inbound connections to PLC management ports at the perimeter.
2. Detection: Search firewall and VPN logs for inbound connections to PLC management ports (EtherNet/IP port 44818, Modbus TCP port 502) from external IP addresses. Review HMI/SCADA audit logs for unauthorized login attempts, credential brute-force patterns, and unexpected control logic changes. Query asset inventory for any Rockwell Automation devices with public IP assignments or direct NAT from internet. Cross-reference against the Censys exposure dataset if your asset management does not have full OT visibility.
3. Eradication: Rotate all PLC and HMI credentials immediately; eliminate any default credentials (CWE-1188). Enforce strong authentication on all OT devices. Apply network segmentation: OT devices must not be reachable from the internet or corporate IT networks without explicit, authenticated, monitored jump-host access. Review and apply all available Rockwell Automation security advisories at https://www.rockwellautomation.com/en-us/trust-center/security-advisories.html for firmware and software hardening guidance.
4. Recovery: After isolation and credential rotation, verify PLC logic integrity by comparing current control logic against known-good baselines. Monitor HMI/SCADA interfaces for anomalous process commands or set-point changes for a minimum of 30 days post-remediation. Validate that no unauthorized logic modifications persist in PLC memory. Confirm OT network segmentation with a firewall rule review and active scanning from the internet side to verify no residual exposure.
5. Post-Incident: Conduct an OT asset inventory review to close visibility gaps that allowed internet-exposed PLCs to persist undetected. Evaluate adoption of CISA's Cross-Sector Cybersecurity Performance Goals (CPGs) for OT environments, specifically network segmentation and remote access controls. Review incident against NIST SP 800-82 (Guide to OT Security) for control gaps. Document findings and schedule a table-top exercise for OT incident response within 90 days.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISA (1-888-282-0870) and senior leadership immediately if active PLC logic modifications, unauthorized set-point changes, or confirmed threat actor presence in OT systems is detected, or if the affected environment serves water/wastewater, power generation, or other Tier 1 critical infrastructure subject to CIRCIA mandatory incident reporting.

Recovery Notes	After restoring network segmentation and rotating credentials, validate PLC logic integrity on every Rockwell ControlLogix, CompactLogix, and MicroLogix device by comparing current .ACD project files against known-good backups using Studio 5000's offline compare function before returning any device to operational control. Maintain enhanced monitoring of EtherNet/IP and Modbus TCP traffic on the OT network segment for a minimum of 30 days, specifically watching for CIP write-class services (service code 0x4D) that indicate set-point manipulation attempts consistent with this Iranian actor campaign. Conduct a full firewall rule audit and external exposure scan at days 7, 14, and 30 post-remediation to confirm no re-exposure of PLC management ports to the internet.
Forensic Artifacts	FactoryTalk Diagnostics logs at C:\ProgramData\Rockwell Automation\FactoryTalk Diagnostics\ on HMI workstations — contain timestamped records of all PLC login events, program download/upload operations, and forced register writes that Iranian actors would generate when modifying control logic or manipulating set-points | RSLinx Classic or RSLinx Enterprise gateway activity logs — record every EtherNet/IP CIP connection request with source IP, target PLC slot, and service type, providing direct evidence of unauthorized remote connections on port 44818 from Iranian infrastructure | Studio 5000 / RSLogix project file (.ACD) exported from PLC flash memory at time of discovery — diff against known-good backup to identify unauthorized ladder logic additions, routine modifications, or tag value changes consistent with process manipulation | Firewall and perimeter router NetFlow or syslog records for TCP port 44818 (EtherNet/IP) and TCP/UDP port 502 (Modbus TCP) — the primary network-layer evidence of Iranian actor reconnaissance and exploitation of internet-exposed PLCs, including session duration, byte counts, and source ASN attribution | PLC controller fault log accessible via Studio 5000 (Controller Properties > General > Controller Log) — records major/minor fault history, mode changes (RUN to PROGRAM), and online edit events that would reflect unauthorized actor interaction with the controller prior to detection

Per-Action IR Details

Containment — Immediately audit all Rockwell Automation and Allen-Bradley PLCs for direct internet exposure. Remove any device from internet-facing network segments or place behind firewall/VPN with deny-all inbound rules. Reference CISA AA26-097A for scope guidance. If isolation is not immediately possible, block all inbound connections to PLC management ports at the perimeter.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy (RS.MA-01: Execute IR plan; isolate affected assets to prevent further manipulation of physical processes)

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST SC-3 (Security Function Isolation), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: For teams without enterprise NAC or next-gen firewalls: run `nmap -sS -p 44818,502,2222,80,443 ` from an external vantage point to confirm exposure before and after firewall changes. Use Windows Firewall (`netsh advfirewall firewall add rule`) or iptables on Linux jump hosts to enforce deny-all inbound on ports 44818 and 502. On Cisco ASA or pfSense (free), create an ACL/rule that explicitly denies any inbound TCP/UDP to the OT VLAN from 0.0.0.0/0. Document the rule change with a timestamp for the incident record.

Evidence: BEFORE isolating, capture the current routing table and ARP cache on any firewall or router fronting the OT segment (`show ip route`, `show arp` on Cisco; `ip route show`, `arp -a` on Linux) to document how the PLC was reachable. Export all current inbound firewall rules and NAT translations to verify which PLC management ports (EtherNet/IP 44818, Modbus TCP 502) were permitted from external IPs. Pull the PLC's current connection table via Studio 5000 Logix Designer or RSLinx Classic — active sessions at time of isolation may identify the threat actor's source IP.

Detection — Search firewall and VPN logs for inbound connections to PLC management ports (EtherNet/IP port 44818, Modbus TCP port 502) from external IP addresses. Review HMI/SCADA audit logs for unauthorized login attempts, credential brute-force patterns, and unexpected control logic changes. Query asset inventory for any Rockwell Automation devices with public IP assignments or direct NAT from internet. Cross-reference against the Censys exposure dataset if your asset management does not have full OT visibility.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis (DE.AE-02: Analyze potentially adverse events; DE.AE-03: Correlate information from multiple sources; DE.CM-01: Monitor networks for adverse events)

Controls: NIST SI-4 (System Monitoring), NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without a SIEM, use `grep` or PowerShell to parse firewall logs: `grep -E ':44818|:502' /var/log/firewall.log | grep ACCEPT` to identify permitted inbound OT protocol connections. For HMI/SCADA audit logs on FactoryTalk View SE, check `C:\ProgramData\Rockwell Automation\FactoryTalk Diagnostics\` for FTDiagnostics log files and parse for failed login events. Run Zeek (free) or Wireshark capture on the OT network span port, filtering `tcp.port == 44818 || tcp.port == 502`, to reconstruct session timelines. Use the Censys free web interface at censys.io to search your organization's public IP ranges for exposed EtherNet/IP banners.

Evidence: Capture FactoryTalk Diagnostics logs from `C:\ProgramData\Rockwell Automation\FactoryTalk Diagnostics\` on the HMI workstation — these record operator login events, logic download/upload events, and forced coil/register writes that an Iranian actor manipulating set-points would generate. Export RSLinx Classic gateway activity logs, which record every EtherNet/IP CIP connection request including source IP and timestamp. Preserve firewall NetFlow or syslog records showing TCP sessions to port 44818 from non-RFC1918 addresses — these are the primary indicator of unauthorized remote PLC access in this campaign.

Eradication — Rotate all PLC and HMI credentials immediately; eliminate any default credentials (CWE-1188). Enforce strong authentication on all OT devices. Apply network segmentation: OT devices must not be reachable from the internet or corporate IT networks without explicit, authenticated, monitored jump-host access. Review and apply all available Rockwell Automation security advisories at https://www.rockwellautomation.com/en-us/trust-center/security-advisories.html for firmware and software hardening guidance.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication (RS.MA-01: Remove threat from environment; eliminate default credentials and unauthorized access paths enabling CWE-1188 exploitation)

Controls: NIST IA-5 (Authenticator Management), NIST SC-7 (Boundary Protection), NIST CM-6 (Configuration Settings), NIST SI-2 (Flaw Remediation), CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software), CIS 5.2 (Use Unique Passwords), CIS 6.5 (Require MFA for Administrative Access)

Compensating: For credential rotation on Rockwell PLCs without centralized identity management: use Studio 5000 Logix Designer to navigate to Controller Properties > Protection and set a new controller password; repeat for every ControlLogix, CompactLogix, and MicroLogix device in inventory. For FactoryTalk Security (the Rockwell IAM layer), use FactoryTalk Administration Console to audit all user accounts, remove any account named 'admin', 'guest', or matching the PLC model number (common default patterns), and enforce minimum 16-character passwords. Document each credential change with timestamp, operator name, and device tag in the incident log per NIST AU-10 (Non-Repudiation).

Evidence: Before rotating credentials, export the full FactoryTalk Security user account list to document which accounts existed (potential evidence of threat-actor-created accounts). Pull the PLC controller log via Studio 5000: Controller Properties > General > Controller Log — this records all program download events, online edits, and fault history, which may show unauthorized logic modifications by the Iranian actors prior to your eradication. Preserve a memory image or ladder logic export (.ACD project file) of the current PLC program state before any changes — this is your forensic baseline for logic tampering analysis.

Recovery — After isolation and credential rotation, verify PLC logic integrity by comparing current control logic against known-good baselines. Monitor HMI/SCADA interfaces for anomalous process commands or set-point changes for a minimum of 30 days post-remediation. Validate that no unauthorized logic modifications persist in PLC memory. Confirm OT network segmentation with a firewall rule review and active scanning from the internet side to verify no residual exposure.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery (RC: Execute recovery plan; restore systems to verified integrity; monitor for recurrence of Iranian actor TTPs post-restoration)

Controls: NIST SI-7 (Software, Firmware, and Information Integrity), NIST CP-10 (System Recovery and Reconstitution), NIST CA-7 (Continuous Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For logic integrity verification without a commercial OT security platform (e.g., Claroty, Dragos): export the current .ACD project file from each ControlLogix/CompactLogix PLC using Studio 5000 offline compare function (`File > Compare Projects`) against your last known-good backup to diff every rung, routine, and tag change. For ongoing process monitoring without a SCADA historian, configure FactoryTalk View SE alarms on all safety-critical set-points (pump speed, valve position, chemical dosing rates) with out-of-band alerting via email or SMS using FactoryTalk Alarms and Events. Re-run `nmap -sS -p 44818,502 ` from an external host weekly for 30 days to confirm no re-exposure.

Evidence: Capture a cryptographic hash (SHA-256 via `certutil -hashfile .ACD SHA256` on Windows) of the verified clean .ACD project file immediately after logic validation — this becomes the new integrity baseline per NIST SI-7 (Software, Firmware, and Information Integrity). Preserve FactoryTalk Diagnostics logs and HMI alarm history for the full 30-day monitoring window; Iranian ICS actors have historically returned to re-compromise systems within days of initial detection (consistent with CISA AA26-097A campaign documentation). Export and archive firewall rule sets with timestamps to demonstrate segmentation was in place during the monitoring period.

Post-Incident — Conduct an OT asset inventory review to close visibility gaps that allowed internet-exposed PLCs to persist undetected. Evaluate adoption of CISA's Cross-Sector Cybersecurity Performance Goals (CPGs) for OT environments, specifically network segmentation and remote access controls. Review incident against NIST SP 800-82 (Guide to OT Security) for control gaps. Document findings and schedule a table-top exercise for OT incident response within 90 days.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity (GV, ID: Lessons learned; update detection capabilities; share intelligence; improve OT visibility to prevent recurrence of Iranian actor targeting via internet-exposed PLCs)

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), NIST PM-28 (Risk Framing), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For OT asset discovery without an enterprise asset management platform: run Shodan Monitor (free tier) against your organization's registered ASN and IP ranges with a saved query for `product:EtherNet/IP` and `port:44818` to surface any re-exposed Rockwell devices. Use Nmap with the `–script enip-info` NSE script against your internal OT VLAN to enumerate all EtherNet/IP-capable devices and build an inventory spreadsheet. For the table-top exercise, use CISA's free Tabletop Exercise Packages (CTEPs) for ICS/OT environments available at cisa.gov — specifically the Water and Wastewater sector package if applicable.

Evidence: Compile the complete incident timeline from firewall logs, FactoryTalk Diagnostics, HMI alarm history, and controller logs into a single chronological record — this is required for CISA voluntary incident reporting (per CIRCIA 2022 reporting obligations if your organization operates critical infrastructure) and serves as the primary input for the lessons-learned meeting. Archive all forensic artifacts (PLC project file exports, network packet captures, credential audit logs) for a minimum of 3 years per NIST AU-11 (Audit Record Retention) to support any future CISA or FBI attribution investigation tied to this Iranian state-affiliated campaign.

Detection Guidance

Priority detection targets: (1) Firewall logs, flag any inbound connection attempts to EtherNet/IP (TCP/UDP 44818), Modbus TCP (502), or CIP ports from external IP space directed at OT network segments. (2) Authentication logs on HMI/SCADA systems, alert on repeated failed login attempts (brute-force pattern consistent with T1110) and successful logins outside of normal operator hours or from unexpected source IPs. (3) PLC change logs, if your historian or SCADA platform records control logic downloads or set-point changes, alert on any such event not tied to a documented change ticket. (4) Network flow data, look for new or unexpected east-west connections between IT and OT network zones, which may indicate lateral movement post-initial access. Behavioral indicators: unexpected process variable changes, HMI alarm floods not correlated with physical plant events, and PLC reboots or mode changes not initiated by operators. No confirmed IOCs (IPs, domains, hashes) are available from verified sources at time of publication; consult CISA AA26-097A directly for any IOCs released in the advisory.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a`	CISA advisory AA26-097A — primary source for campaign IOCs, affected configurations, and mitigation guidance; consult directly for any released indicators	HIGH

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1110** — Brute Force
- **T0855** — Unauthorized Command Message
- **T0816** — Device Restart/Shutdown
- **T0883** — Internet Accessible Device
- **T1133** — External Remote Services
- **T0831** — Manipulation of Control

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-7** — Unsuccessful Logon Attempts
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems

- **SC-7** — Boundary Protection
- **AC-3** — Access Enforcement
- **SC-28** — Protection of Information at Rest

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A01:2021** — Broken Access Control

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.312(d)** — Person or Entity Authentication

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1110	Brute Force	Credential-Access
T0855	Unauthorized Command Message	Impair-Process-Control
T0816	Device Restart/Shutdown	Inhibit-Response-Function
T0883	Internet Accessible Device	Initial-Access
T1133	External Remote Services	Persistence
T0831	Manipulation of Control	Impact

Sources

Source	URL	Tier
Iranian-Affiliated Cyber Actors Exploit Programmable Logic ...	https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a	T1

Source	URL	Tier
Censys warns systemic exposure of Rockwell PLCs enable ...	https://industrialcyber.co/industrial-cyber-attacks/censys-warns-sy...	T3
Rockwell Automation Security Advisories	https://www.rockwellautomation.com/en-us/trust-center/security-advi...	T3
Iranian-affiliated hackers exploited Rockwell Automation ...	https://www.reddit.com/r/PLC/comments/1sfbir4/iranianaffiliated_hac...	T3
Rockwell Automation/Allen-Bradley PLCs	https://www.rescana.com/post/rockwell-automation-allen-bradley-plcs...	T3

Generated 2026-04-13 16:28 UTC by TJS Security Command Center