INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:32 UTC

CISA KEV: Hikvision Cameras + Rockwell Logix OT/ICS Flaws Confirmed Actively Exploited, Deadline March 26 [SCC-2026-0009]

CVE VULNERABILITY | CRITICAL | CVSS 9.8 | CISA KEV

SCC Item ID	SCC-CVE-2026-0005
Type	CVE Vulnerability
CVE ID	CVE-2017-7921, CVE-2021-22681
Severity	CRITICAL
CVSS Base Score	9.8
KEV Status	Yes — CISA Known Exploited Vulnerability (due: 2026-03-26)
Affected Products	Hikvision: Multiple IP camera product lines (older firmware). Rockwell Automation: Studio 5000 Logix Designer, RSLogix 5000, Logix Controllers (multiple versions).
Published	20260306

Executive Summary

Two critical vulnerabilities in widely deployed security cameras and industrial control systems have been confirmed as actively exploited and added to the U.S. government's mandatory patch list. One affects Hikvision IP cameras, some of the most commonly deployed surveillance cameras globally, allowing attackers to access camera feeds and escalate privileges without authentication. The other affects Rockwell Automation's industrial control platform, enabling unauthorized actors on the same network to take control of manufacturing and operational equipment. The timing coincides with heightened geopolitical cyber activity in the Middle East. Organizations operating industrial facilities, surveillance infrastructure, or remote locations with Hikvision cameras should treat remediation as urgent.

Technical Analysis

CISA added CVE-2017-7921 (CVSS 9.8) and CVE-2021-22681 (CVSS 9.8) to the KEV catalog on March 5, 2026 with a remediation deadline of March 26, 2026. CVE-2017-7921 affects Hikvision IP cameras via improper authentication (CWE-287), an unauthenticated attacker can bypass authentication, escalate privileges, and access sensitive data including credentials and camera feeds. CVE-2021-22681 affects Rockwell Automation Studio 5000 Logix Designer and Logix Controllers, unauthenticated network-adjacent actors can bypass authentication to access Logix controllers and manipulate machine configuration or inject code. Geopolitical context: HiatusRAT actors (suspected Iranian nexus) were documented scanning Hikvision devices in a 2024

campaign; the March 2026 KEV addition aligns with elevated OT targeting activity. Rockwell: firmware update alone is insufficient, CISA ICS advisory ICSA-21-056-03 requires compensating controls.

Action Checklist

1. Hikvision cameras:n
2. DETECT, Inventory all Hikvision camera models and firmware versions. Flag devices running firmware prior to security patches.n
3. CONTAIN, Remove Hikvision web management interfaces from internet-accessible exposure immediately.n
4. MITIGATE, Apply available Hikvision firmware updates per vendor security notice.n
5. VERIFY, Audit camera access logs for unauthorized access events.nnRockwell Automation Logix:n
6. DETECT, Inventory all Studio 5000, RSLogix 5000, and Logix Controller instances.n
7. CONTAIN, Restrict network access to Logix controllers to known engineering workstations only. Segment OT network from IT network if not already isolated.n
8. MITIGATE, Apply firmware update AND implement compensating controls per CISA ICS advisory ICSA-21-056-
9. 0
10. Firmware update alone is not sufficient.n
11. VERIFY, Confirm no unauthorized changes to Logix controller configurations during the exposure window.n
12. DEADLINE, March 26, 2026 (federal requirement; treat as immediate for all organizations given active exploitation).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and legal/compliance immediately if: (1) any Hikvision cameras are publicly internet-exposed at patch deadline, (2) any Logix controllers show evidence of unauthorized configuration changes, (3) organization cannot meet March 26 deadline due to technical or resource constraints (federal penalty/notification required), (4) any forensic evidence suggests active attacker presence in OT network.
Recovery Notes	Post-containment: (1) Conduct threat hunt on OT and IT networks for lateral movement artifacts (Zerologon, PrintNightmare exploits commonly follow ICS compromises). (2) Review SCADA historian for any anomalous process parameter changes, setpoint modifications, or valve/motor state changes that could indicate sabotage. (3) Perform post-incident review with engineering team to identify any operational impact (missed alarms, false data, unscheduled downtime) and correlate with forensic timeline. (4) Update security controls documentation and incident response playbook with lessons from this response cycle.

Forensic Artifacts	Hikvision camera audit logs (system events, authentication, configuration changes) — exported from camera web UI or SD card | Camera firmware version history and pre/post-patch firmware binaries (MD5/SHA256 hashes for integrity verification) | Firewall/IDS logs covering external inbound connections to camera IP range (port 80, 443, 8080, 8443) for 90 days prior | Logix controller audit logs and program change history (.ACD baseline comparison, project version control diffs) | Network traffic captures (PCAP files) from OT segment covering Ethernet/IP protocol interactions during exposure window | SCADA HMI operator logs and historian data showing controller state changes and setpoint modifications | Engineering workstation Windows Event Logs (4688 process creation, 4624 logon events) and Rockwell application logs for studio 5000 access | Router/switch configuration change logs and access control list (ACL) modification timestamps | Physical asset inventory tags and serial numbers (cross-reference with logical network inventory for rogue device detection)

Per-Action IR Details

DETECT, Inventory all Hikvision camera models and firmware versions. Flag devices running firmware prior to security patches.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation phase: tools and resources)

Controls: NIST 800-53 CM-8 (Information System Component Inventory), CIS 1.1 (Hardware inventory)

Compensating: Use NMAP with Hikvision-specific fingerprinting: `nmap -p 80,443,8080 --script http-title,ssl-cert | grep -i hikvision`. Cross-reference MAC OUI prefixes (Hikvision uses 08:00:27, 00:05:1F, 58:18:8B). Document in spreadsheet: IP, model (from web UI banner), firmware version (from admin login or RTSP URI), last boot time. Use free tool Shodan CLI if internet-accessible cameras are a concern.

Evidence: Before running inventory: capture baseline network topology (ARP table: `arp -a` on Windows or `arp -n` on Linux). Screenshot each camera's web interface firmware version page. Preserve DHCP server logs showing camera MAC-to-IP mappings for 30 days prior. Document any failed login attempts to camera web interfaces from historical firewall logs.

CONTAIN, Remove Hikvision web management interfaces from internet-accessible exposure immediately.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.2.3 (Containment: short-term measures)

Controls: NIST 800-53 AC-3 (Access Control Enforcement), CIS 6.2 (Network segmentation)

Compensating: Firewall rule (iptables/Windows Firewall): Block inbound TCP 80, 443, 8080, 8443 to camera subnet. Command: `sudo iptables -I INPUT -p tcp --dport 80 -j DROP && sudo iptables -I INPUT -p tcp --dport 443 -j DROP` (Linux); use Windows Firewall with Advanced Security GUI to block inbound on those ports to camera VLAN. If cameras require remote access: implement reverse SSH tunnel from single jump host, not direct internet exposure.

Evidence: Before blocking: capture all inbound connections to camera ports for past 7 days using tcpdump (`sudo tcpdump -i any -w hikvision_pre_block.pcap 'tcp port 80 or tcp port 443 or tcp port 8080'`) or Windows NetFlow. Document source IPs, geolocation (using free MaxMind GeoIP2), and connection frequency. Check firewall logs for any successful authentications or password attempts. Preserve router/firewall configuration before changes.

MITIGATE, Apply available Hikvision firmware updates per vendor security notice.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.2.4 (Eradication: removal of attacker artifacts)

Controls: NIST 800-53 SI-2 (Flaw Remediation), CIS 3.10 (Controlled asset software inventory)

Compensating: If OTA updates fail or firmware is unavailable: implement network-level compensating control—restrict camera access to trusted engineering VLAN only, require VPN authentication for any management access, disable RTSP/HTTP protocols and allow only encrypted HTTPS with certificate pinning on a reverse proxy. Document in change ticket with rollback procedure.

Evidence: Before updating firmware: extract and preserve current firmware version via camera web UI (screenshot or curl to firmware info endpoint). Capture full system configuration export (most cameras support config backup in XML/BIN format—export via admin UI and store securely). Preserve camera system logs for 30 days pre-patch. Document pre-update MD5/SHA256 hash of running firmware if accessible via telnet/SSH. Record boot logs and uptime to establish system state timeline.

VERIFY, Audit camera access logs for unauthorized access events.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.2.5 (Post-Incident Activities: lessons learned) and §3.2.2 (Detection and Analysis: logging requirements)

Controls: NIST 800-53 AU-2 (Audit events), CIS 6.5 (Access control logging)

Compensating: Enable camera audit logging if disabled: access admin UI → System → Logs, enable all authentication and configuration change events, export logs as CSV. If web UI logging is unavailable, capture RTSP and HTTP traffic with Wireshark and filter for authentication attempts: `http.request.method == "POST" && http.request.uri contains "login"`. Check for anomalous user-agent strings or unusual request patterns indicating scripted attacks.

Evidence: Extract camera system event logs (usually stored locally on camera SD card or internal storage—via SFTP or USB export). Search for: (1) failed login attempts (timestamp, source IP if logged), (2) configuration changes (user, timestamp, parameter), (3) privilege escalation events, (4) firmware version changes. Cross-reference with firewall/IDS logs for same timestamp ranges showing suspicious inbound traffic. Preserve raw logs in write-once format (hash and archive). Flag any entries from public IP ranges or unusual geographic origins.

DETECT, Inventory all Studio 5000, RSLogix 5000, and Logix Controller instances.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation: asset inventory)

Controls: NIST 800-53 CM-8 (Information System Component Inventory), CIS 1.1 (Hardware inventory)

Compensating: Use Rockwell Automation's free tool RSLinx Classic or FactoryTalk Services Suite to enumerate controllers on industrial network. Manual: use NMAP to scan for Ethernet/IP protocol on port 2222 (`nmap -p 2222 `). Query Windows registry on engineering workstations for Rockwell install paths: `reg query "HKLM\Software\Rockwell Software"` to locate installed versions. Document: hostname, IP, controller type (L70, L80, CompactLogix, etc.), firmware version (read from controller properties in Studio 5000), last modified date of program (via controller clock), network interfaces (Ethernet/IP, serial).

Evidence: Before inventory scan: capture network baseline of OT segment (ARP table, routing table, active connections). Preserve any existing Rockwell project files with metadata (file modification dates, author, version control history if applicable). Screenshot controller properties panels showing firmware versions. Document physical asset locations and serial numbers. Preserve SCADA HMI logs showing which workstations have accessed controllers in past 90 days.

CONTAIN, Restrict network access to Logix controllers to known engineering workstations only. Segment OT network from IT network if not already isolated.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.2.3 (Containment: short-term measures)

Controls: NIST 800-53 AC-3 (Access Control Enforcement), NIST 800-53 SC-7 (Boundary Protection), CIS 6.2 (Network segmentation)

Compensating: If no VLAN capability: use air-gapped switch or USB serial console for controller management (disconnect Ethernet during updates/config). Implement host-based firewall on engineering workstations (Windows Firewall inbound: allow TCP 2222 only from known controller IPs, deny all else). Use iptables on Linux jump host to proxy access: `sudo iptables -A INPUT -p tcp --dport 2222 -s -j ACCEPT && sudo iptables -A INPUT -p tcp --dport 2222 -j DROP`. Document all engineering workstation MAC/IP addresses and require static IPs.

Evidence: Before segmentation: capture current network traffic on OT segment for 7 days (`tcpdump -i eth0 -w ot_baseline.pcap` or equivalent). Identify all devices currently communicating with Logix controllers (source IPs,

protocols, port usage). Document any non-engineering access attempts (from IT, guest networks, VPN). Preserve firewall/router configuration before changes. Extract any network diagrams from SCADA engineering notes. Log all current network access control lists (ACLs).

MITIGATE, Apply firmware update AND implement compensating controls per CISA ICS advisory. Firmware update alone is not sufficient.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.2.4 (Eradication: removal of attacker artifacts)

Controls: NIST 800-53 SI-2 (Flaw Remediation), NIST 800-53 AC-2 (Account Management for ICS devices)

Compensating: If firmware update is unavailable or high-risk: (1) Implement network Access Control List (ACL) blocking unauthorized source IPs from reaching controller ports. (2) Deploy rate-limiting on Ethernet/IP protocol to prevent brute-force authentication attempts. (3) Enable controller audit logging and forward logs to remote syslog server (many Logix controllers support this via EtherNet/IP gateway). (4) Disable unused Logix controller ports/protocols (disable DDE, disable legacy DF1 if EtherNet/IP is available). (5) Implement application whitelisting on engineering workstations to allow only signed Rockwell Tools.

Evidence: Before firmware update: extract and preserve current Logix controller program (download .ACD file or equivalent via Studio 5000). Capture controller memory state (if possible via online debug). Document all configured I/O modules, network settings, user accounts, and permissions. Take controller backup (most support online backup function). Record firmware version, serial number, MAC address, IP configuration, and module inventory. Preserve pre-update system logs (at least 30 days) showing any unauthorized access attempts or configuration changes. Establish change control ticket with authorized rollback procedure.

VERIFY, Confirm no unauthorized changes to Logix controller configurations during the exposure window.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.2.5 (Post-Incident Activities: validation and lessons learned)

Controls: NIST 800-53 CA-7 (Continuous Monitoring), NIST 800-53 SI-7 (Software, Firmware, and Information Integrity Monitoring)

Compensating: Compare pre-incident and post-incident controller configurations: download current .ACD program from controller via Studio 5000, use text-based diff tool (`diff -u pre_incident.acd post_incident.acd`) to identify any program changes. Manually audit controller memory for unauthorized ladder logic, indirect jumps, or hidden routines (review processor status, user-defined data types, hidden tag additions). Check controller clock/real-time for any tampered timestamps. Review all user account logins in controller audit log (if available) during exposure window—correlate with engineering team shift logs to identify anomalous access.

Evidence: Preserve pre-incident baseline of controller configuration (downloaded .ACD file, configuration spreadsheet, ladder logic comments). Collect all controller audit logs covering full exposure window (from initial vulnerability date to patch application). Extract system event logs from any SCADA HMI that monitored the controller. Capture any historian data showing unexpected parameter changes or I/O state anomalies. Document any maintenance/engineering work performed during exposure window with signed change tickets. Preserve network traffic captures on OT segment during critical exposure period for forensic analysis of any suspicious Ethernet/IP traffic.

DEADLINE, March 26, 2026 (federal requirement; treat as immediate for all organizations given active exploitation).

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation: security policy and incident response plan)

Controls: NIST 800-53 CP-2 (Contingency Planning), NIST 800-53 PM-3 (Information Security Resources)

Compensating: Establish executive escalation timeline: Day 1 (today): notify CISO and business continuity team of deadline. Day 3: inventory completion required. Day 5: containment measures in place (no internet exposure). Day 7: compensating controls deployed if firmware unavailable. Day 14: firmware patching begins (phased if downtime is critical). Day 21: final verification and forensic review complete. If patch conflicts with production systems, document technical exception and escalate to federal compliance officer immediately with alternative compensating control plan.

Evidence: Establish change management and approval documentation for all remediation steps. Document any conflicts between patch requirements and operational uptime (for federal exception requests). Create audit trail: who approved each step, when, signature. Preserve all communications with Hikvision/Rockwell support regarding patch availability and deployment guidance. Create incident log entry with CVE references, affected assets, remediation progress, and sign-off by authorized personnel.

Detection Guidance

Hikvision: Monitor for authentication attempts to camera management interfaces from unexpected source IPs. Alert on default credential use (admin/12345 or similar). Check for unusual network traffic originating from camera subnets. Note: Metasploit modules exist for CVE-2017-7921, this is a well-documented attack surface.nnRockwell Logix: Monitor for unexpected EtherNet/IP connections to Logix controllers from IPs not in the authorized engineering workstation list. Alert on PLC configuration changes outside of authorized change windows. Look for CIP (Common Industrial Protocol) packets originating from non-engineering-workstation hosts. Reference CISA ICS advisory ICSA-21-056-03 for specific detection indicators.

Indicators of Compromise

Type	Value	Context	Confidence
FILE_PATH	`/etc/passwd`	Unauthorized access to /etc/passwd via unauthenticated HTTP requests to Hikvision camera ISAPI endpoint; unexpected when accessed by non-root external processes	HIGH
FILE_PATH	`/etc/shadow`	Suspicious when unauthenticated or non-privileged processes access /etc/shadow on Hikvision cameras exploiting CVE-2017-7921, as legitimate access occurs exclusively through authenticated root operations during password management, whereas this exploit bypasses authentication to exfiltrate credential hashes for lateral movement and credential stuffing - detect in logs via unauthorized file read attempts from web service processes (e.g., lighttpd, nginx), absence of corresponding sudo/su audit entries, and credential hash exfiltration over network channels outside normal administrative channels.	HIGH
FILE_PATH	`/proc/net/tcp`	Attackers exploiting Hikvision cameras may read network connection state from proc filesystem after gaining unauthorized access	MEDIUM

Type	Value	Context	Confidence
FILE_PATH	`/mnt/flash/`	Hikvision camera firmware and configuration files stored in flash mount may be accessed via CVE-2017-7921 exploitation	MEDIUM
FILE_PATH	`/tmp/malware`	Use of /tmp/malware directory on Hikvision camera devices is suspicious when staging files prior to execution or persistence mechanisms, as legitimate camera firmware and services do not write to arbitrarily named malware directories; detection should focus on file creation events in /tmp/malware followed by chmod/chown operations or process execution from this path, which differs from normal camera operations that use manufacturer-defined temporary directories like /tmp or /var/tmp for legitimate logging and cache purposes.	MEDIUM
FILE_PATH	`/var/run/`	Runtime files on Hikvision cameras may be modified by attackers exploiting authentication bypass to persist access	LOW
FILE_PATH	`/home/httpd/`	Hikvision web server root directory targeted during CVE-2017-7921 ISAPI exploitation attempts	HIGH
FILE_PATH	`/Rockwell/RSLogix/`	Rockwell Automation Studio 5000 Logix Designer project files targeted via CVE-2021-22681 CIP cryptographic vulnerability	HIGH
FILE_PATH	`/Program Files (x86)/Rockwell Software/Studio 5000/`	Rockwell Studio 5000 installation directory targeted by CVE-2021-22681 allowing forged CIP connections to Logix controllers	HIGH
FILE_PATH	`/Program Files/Rockwell Software/RSLinx/`	RSLinx Classic installation path relevant to Rockwell Logix CVE-2021-22681 exploitation chain targeting OT communication layer	MEDIUM

Type	Value	Context	Confidence
FILE_PATH	`/var/log/auth.log`	Authentication log file on Hikvision Linux-based cameras that is suspicious when showing repeated failed login attempts followed by successful authentication without corresponding credential entries, or when access patterns indicate CVE-2017-7921 exploitation attempts; legitimate use involves standard SSH/login authentication logging whereas exploitation attempts typically show privilege escalation or unauthenticated access grants coinciding with HTTP request logs showing camera interface manipulation.	MEDIUM
FILE_PATH	`/tmp/`	Suspicious when Hikvision camera processes write executable files, scripts, or binaries to /tmp/ outside of documented firmware update procedures, as legitimate device operations use manufacturer-controlled staging paths; detect via EDR monitoring for unsigned binary writes, script execution from /tmp/, or persistence mechanisms following network connections from external sources, privilege escalation attempts, or unexpected process spawning (e.g., shell interpreters, curl/wget downloads), and differentiate from legitimate firmware staging by confirming writes occur during scheduled updates via authenticated channels rather than spontaneous external connections or unusual parent processes.	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application
- **T1078.001** — Default Accounts
- **T0866** — Exploitation of Remote Services
- **T0835** — Manipulate I/O Image

NIST-800-53R5

- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection

- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity

CIS-V8

- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.23** — Information security for use of cloud services

NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1190	Exploit Public-Facing Application	Initial-Access
T1078.001	Default Accounts	Defense-Evasion
T0866		
T0835		

Sources

Source	URL	Tier
CISA KEV Alert, March 5, 2026	https://www.cisa.gov/news-events/alerts/2026/03/05/cisa-adds-five-k...	T1
The Hacker News	https://thehackernews.com/2026/03/hikvision-and-rockwell-automation...	T3
SOCRadar	https://socradar.io/blog/hikvision-camera-rockwell-logix-cisa/	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2017-7921, CVE-2021-22681	T1
CISA KEV	https://www.cisa.gov/known-exploited-vulnerabilities-catalog	T1

Generated 2026-03-29 18:32 UTC by TJS Security Command Center