INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-30 14:00 UTC

CISA Advisory: Hard-Coded Admin Credentials in USR-W610 IoT Gateway (CVE-2026-7786)

CVE VULNERABILITY | **CRITICAL** | CVSS 9.8

SCC Item ID	SCC-CVE-2026-0241
Type	CVE Vulnerability
CVE ID	CVE-2026-7786
Severity	CRITICAL
CVSS Base Score	9.8
EPSS Score	0.0004 (13th percentile)
Affected Products	Jinan USR IOT Technology Limited PUSR USR-W610 RS232/485 to Wi-Fi/Ethernet converter, firmware version 7.03T.07
Published	2026-05-28
Discovery Source	Gemini

Executive Summary

CISA has issued an advisory for CVE-2026-7786, a critical vulnerability in the Jinan USR IOT Technology Limited PUSR USR-W610 serial-to-network converter affecting firmware version 7.03T.07. The device ships with identical hard-coded administrator credentials across all units, meaning any attacker who obtains those credentials through firmware analysis or public disclosure gains full administrative control over every unpatched device on the network. Organizations running these converters to bridge legacy industrial serial equipment to IP networks face a direct path to operational disruption or industrial asset compromise. As of the analysis date, this vulnerability is not listed in the CISA Known Exploited Vulnerabilities catalog; however, hard-coded credential classes have historically seen rapid public exploitation upon disclosure.

Technical Analysis

CVE-2026-7786 is a CWE-798 (Use of Hard-Coded Credentials) vulnerability in the Jinan USR IOT Technology Limited PUSR USR-W610 RS232/RS485-to-Wi-Fi/Ethernet converter, firmware version 7.03T.07. The device stores static plaintext administrator credentials in firmware, identical across all shipped units. An unauthenticated remote attacker who obtains these credentials via firmware extraction, network traffic capture, or public disclosure can authenticate with full administrative privileges to the device management interface without any additional authorization. MITRE ATT&CK techniques T1133 (External Remote Services), T1552.001

(Credentials In Files), and T1078.001 (Default Accounts) map directly to exploitation paths. The vulnerability is particularly severe in OT/ICS-adjacent deployments where USR-W610 units bridge legacy RS232/RS485 serial equipment to IP networks, creating a potential lateral movement path from IT to operational technology environments. Analyst-derived CVSS base score: 9.8 (Critical). No vendor-supplied CVSS vector was available at analysis time; vector string to be updated upon NVD official publication. EPSS score: 0.00041 (12.94th percentile) indicates low current exploitation probability at time of analysis, though hard-coded credential classes historically see rapid public exploitation once credentials are disclosed. VERIFICATION REQUIRED: NVD record availability for CVE-2026-7786 should be confirmed by the analyst. Authoritative source: CISA advisory referenced in sb26-026 weekly bulletin. CISA KEV listing: not confirmed at analysis time.

Action Checklist

1. Step 1: Containment. Immediately identify all USR-W610 devices running firmware 7.03T.07 on your network using CIS 1.1 asset inventory. Isolate any device with a management interface exposed to untrusted networks by restricting management interface access to a dedicated out-of-band management network segment via access control lists (ACLs). Apply network segmentation per NIST AC-4 (Information Flow Enforcement) to prevent lateral movement from compromised converters into OT/ICS segments.
2. Step 2: Detection. Query firewall and authentication logs for unexpected login attempts or successful logins to USR-W610 management interfaces (typically TCP port 80 for web UI or TCP 23 for Telnet, note: Telnet is an unencrypted legacy protocol; upgrade to SSH or HTTPS if vendor firmware supports it). Flag any administrative session not initiated from a known management workstation IP. Review serial port traffic logs if available; unauthorized configuration changes to connected RS232/RS485 equipment may indicate post-exploitation activity. Apply NIST AU-6 (Audit Record Review, Analysis, and Reporting) procedures. Reference CIS 8.2 (Collect Audit Logs) to confirm logging is enabled on network infrastructure adjacent to these devices.
3. Step 3: Eradication. Check Jinan USR IOT Technology Limited's official support portal for a firmware update that removes or randomizes the hard-coded credentials. If a patched firmware version is available, apply it following the vendor's upgrade procedure. If no patch is available, implement compensating controls: restrict management interface access to a dedicated out-of-band management VLAN, disable web and Telnet management interfaces if the application supports CLI-only access, and change any user-configurable credentials to unique values per device per NIST AC-2 (Account Management) and CIS 5.2 (Use Unique Passwords).
4. Step 4: Recovery. After applying firmware updates or compensating controls, verify the management interface no longer accepts the previously known hard-coded credentials. Conduct a port scan of all USR-W610 devices to confirm management interfaces are no longer externally reachable. Re-audit authentication logs for 72 hours post-remediation to detect any residual unauthorized access attempts. Validate that connected RS232/RS485 serial equipment is operating within expected parameters; confirm no unauthorized configuration changes were made to downstream industrial assets per NIST IR and NIST SI-4 (System Monitoring).
5. Step 5: Post-Incident. Document control gaps this vulnerability exposed: absence of a hard-coded credential detection process in your procurement/vendor assessment workflow, insufficient network segmentation between IT and OT segments, and gaps in IoT/OT device inventory. Update your vendor risk assessment process to require firmware security attestation for all serial-to-network converters and OT boundary devices. Map findings to NIST AC-6 (Least Privilege) and CIS 4.2 (Secure Configuration Process for Network Infrastructure). Consider deploying enhanced local account monitoring on

OT-adjacent network segments and enable alerting for Telnet protocol access.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to senior IR leadership, OT/ICS engineering, and legal/compliance immediately if firewall logs confirm any successful authentication to a USR-W610 management interface from a non-management source IP, if historian or SCADA data shows unexpected setpoint changes on connected serial devices during the exposure window, or if any USR-W610 unit bridges IT and OT segments in an environment subject to NERC CIP, ICS-CERT reporting obligations, or sector-specific OT incident notification requirements.
Recovery Notes	After firmware update or compensating control application, perform a protocol-level integrity check on every RS232/RS485 serial device connected through a USR-W610 unit — read current configuration registers and compare against your last known-good baseline, as an attacker with hard-coded admin access could have modified serial forwarding rules or injected commands to downstream PLCs, RTUs, or meters without leaving a trace on the converter itself. Monitor firewall deny logs and any OT historian anomaly alerts continuously for a minimum of 72 hours post-remediation, extending to 7 days if exploitation is confirmed. If no patched firmware is available from Jinan USR IOT, treat the out-of-band management VLAN isolation and Telnet/web interface disable as permanent controls, not temporary, and initiate a procurement process to replace affected units with devices that meet your firmware security attestation requirements.
Forensic Artifacts	Firewall flow logs (NetFlow, syslog, or ACL hit counters) for TCP/80, TCP/23, and TCP/9999 destined to USR-W610 device IPs — the hard-coded credential exploit requires no brute force, so a single successful session from an unexpected source IP is the primary indicator of compromise for this vulnerability | Packet capture of Telnet sessions to USR-W610 devices (port 23) — Telnet is cleartext, so any capture containing the hard-coded admin username and password followed by configuration commands (e.g., AT+commands or web form POST data to '/goform/') constitutes direct exploitation evidence | USR-W610 configuration export file (retrievable pre-patch via HTTP GET to the device backup endpoint) — compare the serial port forwarding rules, allowed IP list, and management credential hash against your baseline to identify attacker-modified settings | RS232/RS485 serial device logs or SCADA historian records for connected downstream equipment — unauthorized Modbus write function codes (FC06, FC16) or proprietary configuration frames at anomalous timestamps are the primary post-exploitation impact artifact for this serial-to-network converter vulnerability class | HTTP server access logs from any reverse proxy or network tap positioned upstream of the USR-W610 web management interface — POST requests to '/goform/login' with non-management source IPs, followed by subsequent GET requests to configuration or status endpoints, indicate successful credential use and administrative session establishment

Per-Action IR Details

Step 1: Containment — Immediately identify all USR-W610 devices running firmware 7.03T.07 on your network using CIS 1.1 asset inventory. Isolate any device with a management interface exposed to untrusted networks by placing it behind a firewall or disabling remote management access. Apply network segmentation per NIST AC-4 (Information Flow Enforcement) to prevent lateral movement from compromised converters into OT/ICS segments.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST AC-4 (Information Flow Enforcement), NIST IR-4 (Incident Handling), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Run an nmap scan scoped to your OT/IT boundary subnets to fingerprint USR-W610 devices: 'nmap -p 80,23,9999 --open -sV /24 | grep -A5 USR' — TCP/9999 is the USR IOT serial tunneling port that uniquely identifies this product family. Use the resulting IP list to immediately create ACL deny rules on your perimeter or OT firewall blocking inbound TCP 80, 23, and 9999 from untrusted zones. If firewall ACLs are not available, physically disconnect the WAN/LAN Ethernet port and revert to RS232/RS485-only operation for the connected serial device until remediation is complete.

Evidence: Before isolating, capture: (1) a full ARP table dump from the OT network switch ('show arp' or 'arp -a' on adjacent hosts) to document which MAC addresses map to USR-W610 units — USR IOT devices use MAC OUI 00:1A:2B as a common prefix, verify against vendor documentation; (2) a packet capture (tcpdump or Wireshark) on the OT segment for 60 seconds to record any active sessions to TCP/80, TCP/23, or TCP/9999 on identified device IPs — existing sessions indicate live exploitation; (3) screenshot or HTTP GET of the USR-W610 web management page (typically http:///index.html) to confirm firmware version string '7.03T.07' appears in the page header before isolation.

Step 2: Detection — Query firewall and authentication logs for unexpected login attempts or successful logins to USR-W610 management interfaces (typically TCP port 80 or Telnet port 23, depending on firmware configuration). Flag any administrative session not initiated from a known management workstation IP. Review serial port traffic logs if available — unauthorized configuration changes to connected RS232/RS485 equipment may indicate post-exploitation activity. Apply NIST AU-6 (Audit Record Review, Analysis, and Reporting) procedures. Reference CIS 8.2 (Collect Audit Logs) to confirm logging is enabled on network infrastructure adjacent to these devices.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: The USR-W610 itself does not generate syslog by default in firmware 7.03T.07 — rely on adjacent infrastructure: (1) query your perimeter or OT firewall logs for any ACCEPT entries to the device IPs on TCP/80 or TCP/23 from non-management source IPs over the past 30 days; (2) on a Linux host adjacent to the OT segment, run 'tcpdump -i -w usrw610_capture.pcap host and (port 80 or port 23 or port 9999)' and analyze with Wireshark display filter 'http.request.method == POST' to identify credential submission attempts to the web management login endpoint '/goform/login'; (3) if Telnet sessions reached the device, Wireshark filter 'telnet' will show cleartext credential exchanges — the hard-coded admin username documented in the CISA advisory should appear in plaintext in captured Telnet streams.

Evidence: Capture before analysis: (1) firewall flow logs (NetFlow/IPFIX or syslog ACCEPT/DENY records) for all traffic destined to USR-W610 device IPs on TCP/80, TCP/23, TCP/9999 for the maximum available retention window — look for source IPs outside your defined management VLAN; (2) if the device's web server is still reachable, retrieve the current configuration via HTTP GET to 'http:///goform/GetStatus' (a common USR IOT firmware endpoint) before patching, to document the current admin account state and any modified serial port forwarding rules that may indicate post-exploitation reconfiguration; (3) RS232/RS485 serial device command logs from any downstream PLC, RTU, or meter data management system — unauthorized configuration writes via the serial tunnel would appear as unexpected Modbus function codes (FC 06 Write Single Register, FC 16 Write Multiple Registers) or proprietary configuration frames at abnormal timestamps.

Step 3: Eradication — Check Jinan USR IOT Technology Limited's official support portal for a firmware update that removes or randomizes the hard-coded credentials. If a patched firmware version is available, apply it following the vendor's upgrade procedure. If no patch is available, implement compensating controls: restrict management interface access to a dedicated out-of-band management VLAN, disable web and Telnet management interfaces if the application supports CLI-only access, and change any user-configurable credentials to unique values per device (NIST AC-2, Account Management; CIS 5.2, Use Unique Passwords;

D3-CRO, Credential Rotation).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), NIST SI-2 (Flaw Remediation), CIS 5.2 (Use Unique Passwords), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software)

Compensating: As of the CISA advisory date, verify patch availability at the Jinan USR IOT official support site (docs.usr.cn or usr.cn/download) — do not source firmware from third-party repositories. If no patched firmware exists: (1) log into each USR-W610 web management interface using the current admin credentials and change the user-configurable password to a unique 16+ character random string per device, documented in a password manager or encrypted spreadsheet — note that this does NOT eliminate the hard-coded credential if it is burned into firmware at a lower privilege layer; (2) use the device's web UI or AT command interface to disable the Telnet management service and restrict web management access to a single authorized management IP using the device's IP filtering feature (if supported in 7.03T.07); (3) create a VLAN ACL entry that permits TCP/80 only from your OT management workstation IP to each USR-W610 IP, and drops all other management-plane traffic.

Evidence: Before applying firmware or compensating controls, preserve: (1) a full device configuration export via the USR-W610 web interface backup function ('http:///goform/exportConfig' or equivalent) — this documents the pre-remediation state for comparison and any attacker-modified settings; (2) the exact firmware version string from the device web UI or HTTP response headers, confirming you are operating on the vulnerable 7.03T.07 build; (3) a hash (SHA-256) of the current firmware image if extractable, to support later comparison with the vendor-issued patched image and to confirm no unauthorized firmware modification occurred.

Step 4: Recovery — After applying firmware updates or compensating controls, verify the management interface no longer accepts the previously known hard-coded credentials. Conduct a port scan of all USR-W610 devices to confirm management interfaces are no longer externally reachable. Re-audit authentication logs for 72 hours post-remediation to detect any residual unauthorized access attempts. Validate that connected RS232/RS485 serial equipment is operating within expected parameters — confirm no unauthorized configuration changes were made to downstream industrial assets (NIST IR series; NIST SI-4, System Monitoring).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST SI-4 (System Monitoring), NIST IR-4 (Incident Handling), NIST CP-10 (System Recovery and Reconstitution), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Perform a targeted credential verification test before returning each device to service: use curl to attempt login with the known hard-coded credentials against the web management interface — 'curl -s -o /dev/null -w "%{http_code}" -X POST http:///goform/login -d "username=&password="' — a 200 response with session cookie indicates the credential still works and remediation failed; a 401 or redirect to error page confirms rejection. For serial equipment validation, use a protocol-appropriate tool (e.g., ModbusPoll free edition or 'mbpoll' CLI) to read current register values from connected PLCs or RTUs and compare against the last known-good configuration baseline to detect unauthorized parameter changes introduced via the serial tunnel during any exploitation window.

Evidence: After remediation, retain for the 72-hour monitoring window: (1) firewall logs showing all connection attempts to former USR-W610 management ports — any continued probing from external IPs indicates an attacker is aware of the asset and still attempting access post-patch; (2) serial protocol logs or historian data from connected RS232/RS485 devices covering the full suspected exploitation window through 72 hours post-remediation — anomalous setpoint changes, mode switches, or communication errors on downstream industrial equipment are the primary post-exploitation impact indicator for this vulnerability class; (3) the curl-based credential test output for each device, timestamped and logged, as documented evidence of successful eradication.

Step 5: Post-Incident — Document control gaps this vulnerability exposed: absence of a hard-coded credential detection process in your procurement/vendor assessment workflow, insufficient network

segmentation between IT and OT segments, and gaps in IoT/OT device inventory. Update your vendor risk assessment process to require firmware security attestation for all serial-to-network converters and OT boundary devices. Map findings to NIST AC-6 (Least Privilege) and CIS 4.2 (Secure Configuration Process for Network Infrastructure). Consider deploying D3-LAM (Local Account Monitoring) on OT-adjacent network segments.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST AC-6 (Least Privilege), NIST RA-3 (Risk Assessment), NIST SA-9 (External System Services), NIST CM-6 (Configuration Settings), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Add a hard-coded credential check to your procurement checklist for any serial-to-network converter or OT boundary device: require vendors to provide a signed firmware bill of materials (SBOM) and attest in writing that no universal default or hard-coded credentials exist in production firmware — this directly addresses the root cause of CVE-2026-7786. For ongoing detection, deploy a Sigma rule on your log aggregator (even a free ELK stack) alerting on any successful authentication to OT management interfaces from source IPs outside the designated management VLAN: use Sigma rule class 'network_connection' filtering on destination ports 80, 23, and 9999 to your OT subnet. Add USR-W610 and equivalent serial-to-network converter device classes as a standing query category in your quarterly asset inventory review.

Evidence: For the lessons-learned record and any regulatory reporting, preserve: (1) the asset inventory query results showing how many USR-W610 units at firmware 7.03T.07 were present and how long they had been deployed without segmentation controls — this documents the exposure window; (2) a network diagram excerpt showing the IT/OT boundary topology at time of discovery, evidencing the segmentation gap; (3) vendor communications with Jinan USR IOT Technology Limited requesting a patched firmware version and their response timeline — relevant if regulatory reporting of an OT incident requires documentation of remediation due diligence.

Detection Guidance

Primary detection focus: unauthorized authentication to USR-W610 management interfaces. Query firewall logs for inbound connections to known USR-W610 management ports (typically TCP 80 for web UI or TCP 23 for Telnet) from external or unexpected internal IP addresses. Flag Telnet (TCP 23) access as a secondary control gap requiring protocol upgrade to SSH or HTTPS. Flag any successful authentication event not sourced from an approved management VLAN or workstation. If your environment captures device-level syslog from the converters, search for admin login events outside of scheduled maintenance windows. Behavioral indicators of post-exploitation include: unexpected configuration changes to serial port parameters, baud rate, or connected device addressing; unusual outbound connections from the converter's IP address; and changes to the device hostname, NTP server, or SNMP community strings. Because the credentials are static and shared across all units, any public disclosure of the hard-coded values should be treated as an immediate trigger to assume authentication attempts are already occurring. No public IOCs (IPs, domains, hashes) are confirmed for active exploitation of this CVE at analysis time. Apply NIST AU-6 review procedures and ensure CIS 8.2 logging is active on network segments containing these devices.

Framework Mappings

MITRE-ATTACK

- **T1133** — External Remote Services

- **T1552.001** — Credentials In Files
- **T1078.001** — Default Accounts

NIST-800-53R5

- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SC-7** — Boundary Protection

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **6.3** — Require MFA for Externally-Exposed Applications

ISO-27001-2022

- **A.8.28** — Secure coding
- **A.8.8** — Management of technical vulnerabilities

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1133	External Remote Services	Persistence
T1552.001	Credentials In Files	Credential-Access
T1078.001	Default Accounts	Defense-Evasion

Sources

Source	URL	Tier
CVE-2026-7786 - Exploits & Severity - Feedly	https://feedly.com/cve/CVE-2026-7786	T3

Source	URL	Tier
CVE-2026-7786 - Critical Vulnerability - TheHackerWire	https://www.thehackerwire.com/vulnerability/CVE-2026-7786/	T3
CISA Warns CVE-2026-7786: Hard-Coded Admin Credentials in ...	https://windowsforum.com/threads/cisa-warns-cve-2026-7786-hard-code...	T3
CVE-2026-7778 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-7778	T1
Vulnerability Summary for the Week of January 19, 2026 | CISA	https://www.cisa.gov/news-events/bulletins/sb26-026	T1
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-7786	T1

Generated 2026-05-30 14:00 UTC by TJS Security Command Center