INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-05 06:57 UTC

Seven CVEs in Hitachi Energy RTU500 CMU Firmware Expose Critical Infrastructure to DoS and Data Compromise via Third-Party Library Flaws

CVE VULNERABILITY | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CVE-2026-0267
Type	CVE Vulnerability
CVE ID	CVE-2025-69421, CVE-2026-24515, CVE-2026-25210, CVE-2026-32776, CVE-2026-32777, CVE-2026-32778, CVE-2026-8479
Severity	HIGH
CVSS Base Score	7.5
EPSS Score	0.0013 (32th percentile)
Affected Products	Hitachi Energy RTU500 series CMU Firmware versions 12.7.1-12.7.7, 13.5.1-13.5.4, 13.6.1-13.6.3, 13.7.1-13.7.8, 13.8.1
Published	2026-06-04T12:00:00+00:00
Discovery Source	Rss:T2 Gov

Executive Summary

CISA advisory ICSA-26-155-04 discloses seven vulnerabilities in Hitachi Energy RTU500 series CMU firmware, equipment widely deployed in energy, water, and dam operations. The flaws stem from third-party libraries (libexpat, OpenSSL) and a protocol-level weakness in IEC 60870-5-104, enabling unauthenticated denial-of-service and, in the highest-severity case (CVSS 7.8), potential data compromise. A firmware update to version 13.8.2 is available; organizations operating RTU500 devices should prioritize upgrade scheduling given the critical infrastructure context.

Technical Analysis

Seven CVEs affect Hitachi Energy RTU500 CMU firmware across versions 12.7.1-12.7.7, 13.5.1-13.5.4, 13.6.1-13.6.3, 13.7.1-13.7.8, and 13.8.1. Root causes: (1) libexpat defects, CWE-476 null pointer dereference, CWE-190 integer overflow, CWE-835 infinite loop, exploitable via malformed XML parsing; (2) OpenSSL PKCS#12 handling flaws affecting TLS certificate processing; (3) a protocol-level flaw in IEC 60870-5-104 bidirectional channel initialization (BCI) mode. Individual CVE severity: CVE-2026-25210 carries CVSS 7.8 with

confidentiality and integrity impact; remaining six CVEs range from 5.4 to 7.5 CVSS and primarily target availability. MITRE ICS techniques mapped: T0814 (Denial of Service), T1499 (Endpoint Denial of Service), T0816 (Device Restart/Shutdown), T0836 (Modify Parameter), T1190 (Exploit Public-Facing Application), T0846 (Remote System Discovery). EPSS score is low (0.00128, 31st percentile), and the vulnerabilities are not currently listed in CISA KEV. Attack vectors are network-adjacent for the IEC 104 flaw and network-reachable for the library-based issues. No public proof-of-concept exploitation has been disclosed in the source data. Remediation: upgrade to RTU500 CMU firmware version 13.8.2 per CISA advisory ICSA-26-155-04.

Action Checklist

1. Containment: Identify all RTU500 series devices running CMU firmware versions 12.7.1-12.7.7, 13.5.1-13.5.4, 13.6.1-13.6.3, 13.7.1-13.7.8, or 13.8.1. Where firmware upgrade cannot be applied immediately, isolate affected RTU500 devices at the network perimeter: restrict IEC 60870-5-104 (default TCP port 2404) and IEC 61850 (TCP 102/61850) access to authorized SCADA hosts only, using ACLs on the communication front-end or upstream firewall. Reference: CISA ICSA-26-155-04 mitigations section. NIST AC-4 (Information Flow Enforcement) supports this network segmentation action.
2. Detection: Query asset management and OT network monitoring tools for RTU500 CMU firmware version strings in the affected ranges. In your network flow data, look for unexpected or unauthenticated connections to TCP 2404 (IEC 60870-5-104) or TCP 102 from hosts outside your authorized SCADA/EMS network. Monitor for sudden RTU communication loss or unexpected device restarts, which may indicate DoS exploitation of the libexpat or IEC 104 BCI flaws. Enable logging of all communication sessions to/from RTU500 devices where the firmware supports it. Reference: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs).
3. Eradication: Upgrade all affected RTU500 CMU firmware to version 13.8.2, the remediated release identified in CISA advisory ICSA-26-155-04. Coordinate with Hitachi Energy support for firmware delivery and upgrade procedures specific to your RTU500 hardware variant. Verify that firmware integrity is confirmed before and after upgrade using vendor-supplied checksums. Reference: CIS 7.3 (Perform Automated Operating System Patch Management) and CIS 7.4 (Perform Automated Application Patch Management) for process requirements.
4. Recovery: After upgrade, confirm each RTU500 device reports firmware version 13.8.2 through your asset management or SCADA platform. Validate that IEC 60870-5-104 and IEC 61850 communications resume normally with authorized engineering workstations and control systems. Monitor RTU500 devices for at least 72 hours post-upgrade for anomalous behavior, unexpected restarts, or communication errors. Re-enable any services restricted during containment only after upgrade is confirmed. Reference: NIST AU-6 (Audit Record Review, Analysis, and Reporting) for post-change monitoring.
5. Post-Incident: Review your third-party library inventory process: the libexpat and OpenSSL flaws in this advisory are upstream library vulnerabilities that propagated into OT firmware. Assess whether your vendor management program (NIST AC-1, CIS 7.1 Establish and Maintain a Vulnerability Management Process) requires vendors to disclose embedded library versions and CVE exposure. Evaluate your OT network segmentation posture against NIST AC-4 (Information Flow Enforcement) to confirm protocol-level access to RTU devices is restricted to authorized hosts. Document gaps and schedule remediation.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to OT security leadership and CISA if network flow analysis reveals unauthenticated TCP 2404 or TCP 102 connection attempts from unauthorized hosts, if any RTU500 device exhibits unexpected restarts or communication loss consistent with DoS exploitation, or if SCADA data integrity flags suggest the CVSS 7.8 data compromise vector has been triggered — given RTU500 deployment in energy, water, and dam operations, any confirmed exploitation triggers mandatory ICS incident reporting obligations under CIRCIA and applicable sector-specific requirements (NERC CIP for energy).
Recovery Notes	After confirming firmware 13.8.2 on all affected RTU500 CMU devices, validate IEC 60870-5-104 and IEC 61850 session integrity by reviewing SCADA historian data quality and continuity across the upgrade window — specifically check that no telemetry gaps or data substitution events appear that could indicate pre-upgrade exploitation of the CVSS 7.8 data compromise flaw. Maintain the containment ACLs restricting TCP 2404 and TCP 102 to authorized SCADA/EMS hosts as a permanent hardening measure per ICSA-26-155-04 mitigations, not solely as a temporary compensating control. Conduct a 72-hour post-upgrade monitoring period reviewing RTU500 event logs and network flow data daily before declaring full recovery.
Forensic Artifacts	IEC 60870-5-104 session logs from the SCADA communication front-end server showing all peer IP addresses, APDU sequences, and session reset events on TCP 2404 — malformed or oversized APDUs from unauthorized hosts would indicate exploitation attempts against the IEC 104 BCI protocol-level flaw | RTU500 CMU device diagnostic and crash dump files accessible via the Hitachi Energy engineering tool (PCM600 or serial console) — libexpat heap/stack fault conditions or OpenSSL TLS handshake failures would appear as application fault records if the library flaws were triggered by malformed XML or crafted TLS payloads | SCADA historian alarm and event records for each RTU500 device covering the exposure window — unexpected device restart events, communication quality degradation flags, or data substitution markers are the primary operational indicators of DoS or data compromise exploitation of these CMU firmware vulnerabilities | Network packet captures (PCAP) from the OT DMZ interface filtered on TCP 2404 and TCP 102 — preserve pre-containment captures to document any scanning, connection flooding, or malformed protocol payloads sent toward RTU500 devices, which would constitute evidence of active exploitation attempts | RTU500 CMU configuration exports (point lists, communication parameters, protocol settings) taken before and after the firmware upgrade window — comparison of pre- and post-upgrade configurations can reveal unauthorized configuration changes that would indicate the CVSS 7.8 data compromise vector was exploited prior to remediation

Per-Action IR Details

Containment — Identify all RTU500 series devices running CMU firmware versions 12.7.1–12.7.7, 13.5.1–13.5.4, 13.6.1–13.6.3, 13.7.1–13.7.8, or 13.8.1. Where firmware upgrade cannot be applied immediately, isolate affected RTU500 devices at the network perimeter: restrict IEC 60870-5-104 (default TCP port 2404) and IEC 61850 (TCP 102/61850) access to authorized SCADA hosts only, using ACLs on the communication front-end or upstream firewall. Reference: CISA ICSA-26-155-04 mitigations section. NIST AC-4 (Information Flow Enforcement) supports this network segmentation action.

NIST Phase: Containment

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

Controls: NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Use netstat or ss on the communication front-end host to enumerate active TCP 2404 and TCP 102 sessions before blocking: 'ss -tnp | grep -E "2404|102"'. Apply iptables ACL rules to drop traffic to TCP 2404 from any source not in the authorized SCADA/EMS host list: 'iptables -I INPUT -p tcp --dport 2404 ! -s -j DROP'. On Windows-based front-end hosts, use Windows Firewall with Advanced Security (wf.msc) inbound rules scoped to authorized source IPs. Capture a snapshot of current connection state with Wireshark on the OT DMZ interface before applying ACLs to preserve pre-containment network baseline.

Evidence: Before isolating, capture and preserve: (1) full netflow or packet capture from the OT network segment containing RTU500 devices on TCP 2404 and TCP 102 — specifically any connection attempts from hosts outside the authorized SCADA IP range, which would indicate scanning or exploit attempts against the IEC 60870-5-104 BCI flaw; (2) RTU500 CMU device logs and communication session logs from the communication front-end server showing all peer IP addresses that established IEC 104 sessions; (3) firewall/ACL rule tables as-is before modification, to document pre-containment exposure posture.

Detection — Query asset management and OT network monitoring tools for RTU500 CMU firmware version strings in the affected ranges. In your network flow data, look for unexpected or unauthenticated connections to TCP 2404 (IEC 60870-5-104) or TCP 102 from hosts outside your authorized SCADA/EMS network. Monitor for sudden RTU communication loss or unexpected device restarts, which may indicate DoS exploitation of the libexpat or IEC 104 BCI flaws. Enable logging of all communication sessions to/from RTU500 devices where the firmware supports it. Reference: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs).

NIST Phase: Detection Analysis

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

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 8.2 (Collect Audit Logs), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Use nmap with service version detection to identify RTU500 devices and banner firmware versions across the OT network segment: 'nmap -sV -p 2404,102 -oN rtu500_scan.txt'. Parse results for version strings matching the affected CMU firmware ranges (12.7.1–12.7.7, 13.5.1–13.5.4, 13.6.1–13.6.3, 13.7.1–13.7.8, 13.8.1). For network flow analysis without a SIEM, run Wireshark or tcpdump on the OT DMZ interface filtering on 'tcp port 2404 or tcp port 102' and export to a PCAP for manual review: 'tcpdump -i -w rtu500_traffic.pcap tcp port 2404 or tcp port 102'. Review RTU500 communication front-end logs (typically stored in the SCADA historian or front-end application logs) for session resets, connection floods, or XML parsing errors indicative of malformed libexpat payloads.

Evidence: Preserve before analysis: (1) RTU500 CMU firmware version strings as reported by the asset management platform or SCADA engineering tool — confirm against the affected version list in ICSA-26-155-04; (2) communication front-end application logs showing IEC 60870-5-104 session establishment and termination events, specifically repeated TCP resets or abnormal APDU sequences on TCP 2404 that could indicate IEC 104 BCI exploitation attempts; (3) SCADA historian or alarm logs showing RTU500 communication loss events, unexpected device resets, or data quality flags that correlate with DoS exploitation of the libexpat or OpenSSL flaws; (4) any XML configuration files parsed by the RTU500 CMU (libexpat processes XML — malformed XML payloads would appear in application error logs or crash dumps on the device).

Eradication — Upgrade all affected RTU500 CMU firmware to version 13.8.2, the remediated release identified in CISA advisory ICSA-26-155-04. Coordinate with Hitachi Energy support for firmware delivery and upgrade procedures specific to your RTU500 hardware variant. Verify that firmware integrity is confirmed before and after upgrade using vendor-supplied checksums. Reference: CIS 7.3 (Perform Automated Operating System Patch Management) and CIS 7.4 (Perform Automated Application Patch Management) for process requirements.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 7.2 (Establish and Maintain a Remediation Process), NIST SI-2 (Flaw

Remediation)

Compensating: For teams without automated OT patch management, create a manual firmware upgrade tracker spreadsheet listing each RTU500 device by hostname, IP, hardware variant, current firmware version, and upgrade status. Download the CMU firmware 13.8.2 image from Hitachi Energy's secure portal and verify the SHA-256 or MD5 checksum against the value published in ICSA-26-155-04 before staging: 'sha256sum '. Stage upgrades during a planned maintenance window coordinated with grid operations — RTU500 firmware upgrades typically require a device restart that will interrupt IEC 104 telemetry. Retain the pre-upgrade firmware image and a full configuration backup per Hitachi Energy's RTU500 Firmware Upgrade Application Note before applying.

Evidence: Before upgrading, preserve: (1) a full configuration export from each RTU500 CMU using the Hitachi Energy RTU500 engineering tool (PCM600 or equivalent), capturing current point lists, communication parameters, and protocol settings — this baseline is required to detect any configuration tampering that may have occurred if the device was previously exploited via the CVSS 7.8 data compromise vector; (2) vendor-supplied checksum for the currently installed (vulnerable) firmware version to confirm firmware integrity was not altered; (3) any RTU500 device diagnostic logs or crash dump files accessible via the engineering tool or serial console, which would record libexpat or OpenSSL library fault conditions if exploitation occurred prior to upgrade.

Recovery — After upgrade, confirm each RTU500 device reports firmware version 13.8.2 through your asset management or SCADA platform. Validate that IEC 60870-5-104 and IEC 61850 communications resume normally with authorized engineering workstations and control systems. Monitor RTU500 devices for at least 72 hours post-upgrade for anomalous behavior, unexpected restarts, or communication errors. Re-enable any services restricted during containment only after upgrade is confirmed. Reference: NIST AU-6 (Audit Record Review, Analysis, and Reporting) for post-change monitoring.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: After firmware upgrade, re-query each RTU500 device using the SCADA engineering tool or nmap service version scan to confirm firmware 13.8.2 is active: 'nmap -sV -p 2404 '. Run a 72-hour tcpdump capture on the OT DMZ interface post-upgrade to baseline normal IEC 104 APDU traffic patterns and confirm no abnormal session resets or unexpected peers appear: 'tcpdump -i -w post_upgrade_baseline.pcap tcp port 2404'. Review RTU500 alarm and event logs in the SCADA historian daily for the 72-hour watch period for any restart events, communication quality degradation, or data integrity flags that were not present before the upgrade.

Evidence: Capture during recovery validation: (1) firmware version confirmation screenshots or exported reports from the SCADA asset management platform for each RTU500 device showing version 13.8.2 — retain as compliance evidence against ICSA-26-155-04 remediation requirements; (2) IEC 60870-5-104 session logs from the communication front-end for the 72-hour post-upgrade window, confirming only authorized SCADA/EMS hosts appear as IEC 104 peers; (3) RTU500 event/alarm logs from the SCADA historian covering the upgrade window and 72-hour monitoring period, to document any post-upgrade anomalies and confirm clean recovery.

Post-Incident — Review your third-party library inventory process: the libexpat and OpenSSL flaws in this advisory are upstream library vulnerabilities that propagated into OT firmware — assess whether your vendor management program (NIST AC-1, CIS 7.1 Establish and Maintain a Vulnerability Management Process) requires vendors to disclose embedded library versions and CVE exposure. Evaluate your OT network segmentation posture against NIST AC-4 (Information Flow Enforcement) to confirm protocol-level access to RTU devices is restricted to authorized hosts. Document gaps and schedule remediation.

NIST Phase: Post Incident

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

Controls: NIST AC-1 (Policy And Procedures), NIST AC-4 (Information Flow Enforcement), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Conduct a tabletop review with the OT engineering and vendor management teams using the ICSA-26-155-04 advisory as the case study. Build a software bill of materials (SBOM) request template for Hitachi Energy and other OT vendors, specifically requiring disclosure of libexpat, OpenSSL, and other third-party library versions embedded in firmware, mapped to known CVEs. Use the free CIS Controls Self-Assessment Tool (CIS CSAT) to score your current OT vulnerability management and network segmentation posture and document gaps. Update your OT asset inventory (spreadsheet or osquery-based) to include firmware version tracking fields enabling faster identification in future advisories affecting the same version ranges.

Evidence: Collect and retain as lessons-learned documentation: (1) the pre-incident asset inventory state showing which RTU500 devices were running vulnerable CMU firmware versions — this gap analysis demonstrates detection latency and informs inventory process improvement; (2) a record of the timeline from ICSA-26-155-04 publication to device identification, ACL application, and firmware upgrade completion for each affected RTU500 — used to measure mean time to contain and remediate for OT assets; (3) any vendor communications from Hitachi Energy regarding the libexpat and OpenSSL library versions embedded in CMU firmware across the affected version ranges, to establish a baseline for future SBOM requirements in OT vendor contracts.

Detection Guidance

Primary detection approach is asset-based: query your OT asset inventory or network discovery tool for RTU500 CMU firmware version strings matching 12.7.1-12.7.7, 13.5.1-13.5.4, 13.6.1-13.6.3, 13.7.1-13.7.8, or 13.8.1. If your OT monitoring platform (e.g., Claroty, Dragos, Nozomi) passively fingerprints IEC 60870-5-104 or IEC 61850 traffic, filter for RTU500 device identifiers and cross-reference firmware versions. Behavioral indicators: unexpected RTU500 device restarts or communication dropouts may indicate exploitation of the DoS-class vulnerabilities (libexpat null pointer dereference, integer overflow, or infinite loop). In network flow logs, flag any IEC 104 sessions (TCP 2404) originating from hosts outside your authorized SCADA/EMS IP ranges. Based on available analysis of CISA advisory ICSA-26-155-04, no IOC hashes, IPs, or domains are currently published for these vulnerabilities. EPSS score (0.00128) reflects low observed exploitation probability at time of publication; absence from CISA KEV corroborates no confirmed in-the-wild exploitation. Reference: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs).

Framework Mappings

MITRE-ATTACK

- **T0814** — Denial of Service
- **T1499** — Endpoint Denial of Service
- **T0816** — Device Restart/Shutdown
- **T0836** — Modify Parameter
- **T1190** — Exploit Public-Facing Application
- **T0846** — Remote System Discovery

NIST-800-53R5

- **SC-5** — Denial-of-Service Protection
- **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
- **SI-16** — Memory Protection
- **SR-2** — Supply Chain Risk Management Plan
- **SC-13** — Cryptographic Protection

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management
- **15.1** — Establish and Maintain an Inventory of Service Providers

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain
- **A.5.23** — Information security for use of cloud services

NIST-CSF-2

- **GV.SC-01** — Cybersecurity supply chain risk management program

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners

HIPAA-SECURITY

- **164.312(e)(1)** — Transmission Security

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T0814	Denial of Service	Inhibit-Response-Function
T1499	Endpoint Denial of Service	Impact
T0816	Device Restart/Shutdown	Inhibit-Response-Function
T0836	Modify Parameter	Impair-Process-Control
T1190	Exploit Public-Facing Application	Initial-Access
T0846	Remote System Discovery	Discovery

Sources

Source	URL	Tier
ICS Advisories	https://www.cisa.gov/news-events/ics-advisories/icsa-26-155-04	T1
	https://industrialcyber.co/cisa/hardware-vulnerabilities-in-hitachi...	T3
	https://www.hitachienergy.com/news-and-events/product-releases/2018...	T3
	https://www.hitachienergy.com/news-and-events/product-releases/2020...	T3
April 2026 CVE Landscape - Recorded Future	https://www.recordedfuture.com/blog/april-cve-landscape	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2025-69421, CVE-2026-24515, CV...	T1

Generated 2026-06-05 06:57 UTC by TJS Security Command Center