INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-18 14:16 UTC

Rockwell FactoryTalk Historian SE Carries Authentication Bypass and DoS Flaws Across OT Environments

CVE VULNERABILITY | HIGH | CVSS 7.5

SCC Item ID	SCC-CVE-2026-0325
Type	CVE Vulnerability
CVE ID	CVE-2025-13036, CVE-2025-44019, CVE-2025-36539
Severity	HIGH
CVSS Base Score	7.5
EPSS Score	0.0028 (20th percentile)
Affected Products	Rockwell Automation FactoryTalk Historian Site Edition (SE), versions 11.00 and earlier
Published	2026-06-18T12:00:00+00:00
Discovery Source	Rss:T2 Gov

Executive Summary

CISA and Rockwell Automation disclosed three vulnerabilities in FactoryTalk Historian Site Edition (versions 11.00 and earlier), including an authentication bypass rated CVSS 9.2 that requires no credentials and is exploitable over the network. Organizations running this historian in manufacturing or industrial control environments face unauthorized access to time-series process data and potential disruption of OT operations. No active exploitation has been reported, but the network-accessible attack vector elevates urgency for any site without strong OT network segmentation.

Technical Analysis

Three vulnerabilities affect Rockwell Automation FactoryTalk Historian SE, versions 11.00 and earlier, disclosed via CISA ICS Advisory ICSA-26-169-03 and NVD. CVE-2025-13036 (CWE-287, CVSS 9.2) is an authentication bypass exploitable over the network with no authentication required, enabling unauthorized read and write access to historian process data; MITRE ATT&CK mappings include T1078 (Valid Accounts), T1110 (Brute Force), and T1190 (Exploit Public-Facing Application). CVE-2025-44019 (CWE-248, uncaught exception) enables denial-of-service conditions against the historian service, mapped to T1499 (Endpoint Denial of Service) in the Enterprise framework and equivalent to the ICS tactic Impact (denial of service and device restart/shutdown). CVE-2025-36539 (CWE-362, race condition) can be exploited to disrupt or manipulate

historian operations. EPSS score is 0.00284 (19.99th percentile), indicating low probability of exploitation in the current threat landscape relative to other published vulnerabilities; the CVEs are not currently listed in the CISA KEV catalog. Vendor patch status and specific patch IDs should be confirmed directly against the CISA advisory and Rockwell's product portal, as the provided source data does not include a discrete patch version number.

Action Checklist

1. Step 1: Containment, Immediately verify network segmentation for all FactoryTalk Historian SE instances running version 11.00 or earlier. Block inbound network access to historian ports from untrusted segments using perimeter and host-based firewalls per CIS 4.4 (Implement and Manage a Firewall on Servers) and CIS 4.5 (Implement and Manage a Firewall on End-User Devices). If Historian SE is internet-facing or reachable from IT networks without a DMZ, isolate the host until patching is complete. Reference CISA ICS Advisory ICSA-26-169-03 for Rockwell-specific network hardening guidance.
2. Step 2: Detection, Audit authentication logs on FactoryTalk Historian SE hosts for unauthenticated or anomalous access attempts targeting historian service ports. Query SIEM for events matching historian service process names with failed or missing authentication fields (AU-6, Audit Record Review, Analysis, and Reporting). Enable logging per CIS 8.2 (Collect Audit Logs) if not already active. Look for unexpected historian service crashes or restarts as indicators of CVE-2025-44019 DoS exploitation. Monitor for race-condition artifacts such as inconsistent data writes or process thread errors in application logs consistent with CVE-2025-36539.
3. Step 3: Eradication, Apply Rockwell Automation's official patch for FactoryTalk Historian SE as documented in CISA ICS Advisory ICSA-26-169-03 (https://www.cisa.gov/news-events/ics-advisories/icsa-26-169-03) and Rockwell's product security portal (https://www.rockwellautomation.com/en-us/company/news/security.html). Verify the specific patch version and upgrade path directly from these sources, as patch IDs may vary by deployment. Enforce upgrade to a version above 11.00 per CIS 7.3 (Perform Automated Operating System Patch Management) and CIS 7.4 (Perform Automated Application Patch Management).
4. Step 4: Recovery, After patching, verify the historian service authenticates all connections and rejects unauthenticated requests. Confirm service stability under normal load to validate remediation of CVE-2025-44019 DoS conditions. Review historian data integrity for any unauthorized reads or writes that may have occurred during the exposure window. Restore network access incrementally, validating firewall rules and segment controls before re-opening historian ports to adjacent OT zones.
5. Step 5: Post-Incident, Conduct a control gap review against NIST AC-3 (Access Enforcement) and AC-6 (Least Privilege) to assess whether historian access is scoped to only authorized OT users and processes. Review OT network segmentation architecture and document compensating controls for any historian instances that cannot be immediately patched due to operational constraints. Establish a recurring patch review cycle per CIS 7.1 (Establish and Maintain a Vulnerability Management Process) and CIS 7.2 (Establish and Maintain a Remediation Process) that explicitly includes ICS/OT software components.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to OT security leadership and plant operations management immediately if: (1) historian service logs show any authenticated or unauthenticated session originating from outside the OT network segment during the exposure window, indicating potential exploitation of CVE-2025-13036's network-accessible authentication bypass; (2) historian data archives show unauthorized tag writes or reads during the exposure window, which may constitute a reportable OT data integrity event under sector-specific regulations (e.g., NERC CIP for electric utilities); or (3) the FactoryTalk Historian SE instance cannot be isolated or patched within 24 hours due to operational constraints, requiring formal risk acceptance at the plant or CISO level.
Recovery Notes	After applying the Rockwell Automation patch and restoring network access to FactoryTalk Historian SE, maintain heightened monitoring of historian service authentication logs and application event logs for a minimum of 72 hours under production load to confirm CVE-2025-44019 DoS stability and CVE-2025-36539 race-condition behavior are fully resolved. Conduct a historian tag data integrity spot-check covering the full exposure window (from the date the vulnerable version was deployed to the date the host was isolated or patched) by comparing historian archive values against DCS or PLC source records for high-criticality process tags. If discrepancies are identified between historian-recorded values and DCS source records, treat the scope as a potential data integrity incident and engage OT engineering to assess operational impact before returning the historian to full production use.
Forensic Artifacts	FactoryTalk Historian SE application event logs at `%ProgramData%\OSIsoft\` and Windows Application Event Log: contains historian service crash records (Event ID 7034) indicative of CVE-2025-44019 DoS exploitation and authentication error records relevant to CVE-2025-13036 bypass attempts. | Historian archive (.arc) and snapshot (.snp) files in the FactoryTalk Historian data directory: examine for tag entries with write timestamps during the exposure window that do not correspond to authorized DCS/PLC source writes, which would indicate unauthorized data manipulation via the CVE-2025-13036 unauthenticated access path. | Windows Security Event Log (Event IDs 4624, 4625, 4648) scoped to the historian service account: unauthenticated or NTLM Type 3 network logon events with no associated Kerberos ticket against the historian host during the exposure window are high-confidence indicators of CVE-2025-13036 exploitation. | Network packet captures from the historian host NIC or upstream SPAN port filtered to historian service ports (default OSIsoft PI: TCP 5450, 5463): sessions with no authentication handshake or anomalous connection teardown patterns are artifacts of the authentication bypass and potential DoS probe activity. | Windows Registry key `HKLM\SOFTWARE\OSIsoft\` and FactoryTalk Historian SE installer logs: preserve pre-patch version strings and installation timestamps to establish the exposure window start date and confirm the installed version (11.00 or earlier) for chain-of-custody documentation.

Per-Action IR Details

Step 1: Containment — Immediately verify network segmentation for all FactoryTalk Historian SE instances running version 11.00 or earlier. Block inbound network access to historian ports from untrusted segments using perimeter and host-based firewalls per CIS 4.4 (Implement and Manage a Firewall on Servers) and CIS 4.5 (Implement and Manage a Firewall on End-User Devices). If Historian SE is internet-facing or reachable from IT networks without a DMZ, isolate the host until patching is complete. Reference CISA ICS Advisory ICSA-26-169-03 for Rockwell-specific network hardening guidance.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: Choose a containment strategy; contain the incident

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 Windows Firewall (netsh advfirewall) or iptables/nftables to block TCP/UDP on OSIsoft PI Server default ports (5450, 5463) and any custom historian service ports identified in the FactoryTalk Historian SE service configuration. Run `netstat -ano | findstr LISTENING` on the historian host to enumerate all bound ports before applying rules. For network-level blocking on a budget, configure ACLs on the nearest managed switch or router to drop traffic from IT VLANs to the historian host IP.

Evidence: Before isolating or applying firewall rules, capture volatile network state: run `netstat -ano` and `Get-NetTCPConnection` on the historian host to document all active inbound sessions to historian service ports — CVE-2025-13036 (CVSS 9.2) requires no credentials, so any established session from an untrusted IP is a high-confidence indicator of unauthorized access. Export `ipconfig /all` and `arp -a` to preserve network context. Capture running process list via `tasklist /svc` to identify any historian child processes or injected services spawned through the bypass. Save output to a write-once location before any firewall change alters active connection state.

Step 2: Detection — Audit authentication logs on FactoryTalk Historian SE hosts for unauthenticated or anomalous access attempts targeting historian service ports. Query SIEM for events matching historian service process names with failed or missing authentication fields (AU-6, Audit Record Review, Analysis, and Reporting). Enable logging per CIS 8.2 (Collect Audit Logs) if not already active. Look for unexpected historian service crashes or restarts as indicators of CVE-2025-44019 DoS exploitation. Monitor for race-condition artifacts such as inconsistent data writes or process thread errors in application logs consistent with CVE-2025-36539.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Analyze all available precursors and indicators; look for correlating information

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-2 (Event Logging), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, use PowerShell to scrape the FactoryTalk Historian SE application event log: `Get-WinEvent -LogName Application | Where-Object { $_.ProviderName -like '*Historian*' -or $_.ProviderName -like '*OSIsoft*' } | Select-Object TimeCreated, Id, Message | Export-Csv historian_events.csv`. Review Windows Security Event Log for Event ID 4625 (failed logon) and Event ID 4624 (successful logon) against the historian service account — unexpected Type 3 (network) logons with no Kerberos ticket (NTLM or anonymous) are consistent with CVE-2025-13036 bypass behavior. Use Wireshark on a mirror/SPAN port to capture traffic to historian ports and filter for sessions with no authentication handshake (`tcp.port == 5450 && !kerberos`).

Evidence: Collect FactoryTalk Historian SE application logs from `%ProgramData%\OSIsoft\` and the Windows Application Event Log before any service restart — CVE-2025-44019 DoS exploitation will produce crash records and service restart entries (Event ID 7034 — Service Control Manager) that are overwritten on restart. Capture Windows Security Event Log entries for the historian service account. For CVE-2025-36539 race-condition exploitation, examine historian archive files for timestamp discontinuities or duplicate tag writes in the `.arc` and `.snp` snapshot files in the FactoryTalk Historian data directory, which indicate concurrent write collisions during exploitation.

Step 3: Eradication — Apply Rockwell Automation's official patch for FactoryTalk Historian SE as documented in CISA ICS Advisory ICSA-26-169-03 and Rockwell's product security portal. The specific patch version and upgrade path must be confirmed directly from Rockwell's advisory, as the source data does not enumerate a discrete patch ID. Enforce upgrade to a version above 11.00 per CIS 7.3 (Perform Automated Operating System Patch Management) and CIS 7.4 (Perform Automated Application Patch Management).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: Eliminate components of the incident; mitigate exploited vulnerabilities

Controls: NIST SI-2 (Flaw Remediation), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: If the Rockwell patch cannot be applied immediately due to OT change-control windows, enforce authentication at the network boundary: require all historian client connections to traverse a jump server with MFA, and document the compensating control formally per your risk acceptance process. Verify the historian service account is

not a local administrator and is scoped to the minimum permissions required by FactoryTalk Historian SE. Record the unpatched version (`11.00` or earlier) in your asset inventory with a tracked exception and a target remediation date.

Evidence: Before applying the patch or upgrading the FactoryTalk Historian SE installation, acquire a full memory image of the historian host using WinPmem or Magnet RAM Capture to preserve any in-memory artifacts of CVE-2025-13036 authentication bypass (e.g., unauthenticated session handles, injected thread state). Take a file-system snapshot or image of the historian data directory — including `.arc`, `.snp`, and configuration files — to preserve evidence of any unauthorized data reads or writes that occurred during the exposure window. Record the pre-patch software version from `HKLM\SOFTWARE\OSIsoft\` or the Rockwell FactoryTalk installer registry keys before the upgrade overwrites them.

Step 4: Recovery — After patching, verify the historian service authenticates all connections and rejects unauthenticated requests. Confirm service stability under normal load to validate remediation of CVE-2025-44019 DoS conditions. Review historian data integrity for any unauthorized reads or writes that may have occurred during the exposure window. Restore network access incrementally, validating firewall rules and segment controls before re-opening historian ports to adjacent OT zones.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: Restore systems to normal operation; confirm systems are functioning normally; implement additional monitoring

Controls: NIST AC-3 (Access Enforcement), NIST SI-2 (Flaw Remediation), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Without an enterprise monitoring stack, validate authentication enforcement manually: attempt a connection to the patched historian service from a test client using no credentials or a deliberately invalid account and confirm the connection is rejected (historian returns an authentication error rather than data). Use Wireshark on the historian host NIC to confirm no unauthenticated sessions are established post-patch. For data integrity validation, compare current historian tag values against a known-good baseline export (OSIsoft DataLink or PI SDK query) from before the exposure window and flag any tag values with write timestamps matching the exploitation window.

Evidence: Before re-opening historian ports to adjacent OT zones, capture a fresh `netstat -ano` and Windows Security Event Log snapshot to establish a clean-state baseline. Monitor FactoryTalk Historian SE application logs for Event ID 7034 recurrence (service instability indicating incomplete DoS remediation for CVE-2025-44019) during the first 24–48 hours of restored operation under production load. Retain the pre-patch archive snapshot and memory image for a minimum of 90 days to support any future forensic review of unauthorized data access during the exposure window.

Step 5: Post-Incident — Conduct a control gap review against NIST AC-3 (Access Enforcement) and AC-6 (Least Privilege) to assess whether historian access is scoped to only authorized OT users and processes. Review OT network segmentation architecture and document compensating controls for any historian instances that cannot be immediately patched due to operational constraints. Establish a recurring patch review cycle per CIS 7.1 (Establish and Maintain a Vulnerability Management Process) and CIS 7.2 (Establish and Maintain a Remediation Process) that explicitly includes ICS/OT software components.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Lessons learned; update detection, policies, and controls based on incident findings

Controls: NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: For teams without a dedicated OT vulnerability management program, establish a manual quarterly review process: subscribe to CISA ICS-CERT advisories (https://www.cisa.gov/ics-advisories) and Rockwell Automation's product security notifications, and map each advisory against a maintained spreadsheet inventory of FactoryTalk Historian SE version and host. Use CIS Controls v8 IG1 safeguards as the baseline checklist for each ICS host review. Document all historian instances still on version 11.00 or earlier with named owners and tracked exception expiry dates.

Evidence: Compile the full incident artifact package for the lessons-learned review: historian application logs, pre- and post-patch network captures, Windows Security Event Log exports covering the exposure window, and the historian archive snapshot. Use these artifacts to determine whether CVE-2025-13036 was probed or exploited during the exposure window by correlating unauthenticated session records with historian tag write timestamps — this distinction (probed vs. exploited) drives the scope of any OT data integrity investigation and regulatory notification assessment. Retain all artifacts per your documented retention policy before closing the incident record.

Detection Guidance

Primary detection focus is CVE-2025-13036 (authentication bypass). Query SIEM and historian application logs for connections to FactoryTalk Historian SE service ports that succeed without an authentication event preceding them, or where authentication fields are null or absent (aligns with AU-3, Content of Audit Records, which requires logging of who, what, when, and where for each event). Alert on repeated historian service crashes or unexpected process terminations as indicators of CVE-2025-44019 exploitation. For CVE-2025-36539 (race condition), look for write conflicts, data inconsistencies, or thread-level errors in historian application logs. D3FEND countermeasure D3-LAM (Local Account Monitoring) applies: monitor historian host accounts for unauthorized local access patterns. D3-SFA (System File Analysis) applies: monitor historian configuration and authentication database files for unauthorized modification. No public IOCs or exploit signatures were present in the source data at time of disclosure; behavioral detection is the primary mechanism until signatures are published.

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1110** — Brute Force
- **T0814** — Denial of Service
- **T0883** — Internet Accessible Device
- **T1499** — Endpoint Denial of Service
- **T1190** — Exploit Public-Facing Application

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
- **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
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **SI-16** — Memory Protection
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

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

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **16.10** — Apply Secure Design Principles in Application Architectures

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC6.3** — Authorizes, modifies, or removes access

HIPAA-SECURITY

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

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
T1078	Valid Accounts	Defense-Evasion
T1110	Brute Force	Credential-Access
T0814	Denial of Service	Inhibit-Response-Function
T0883	Internet Accessible Device	Initial-Access
T1499	Endpoint Denial of Service	Impact
T1190	Exploit Public-Facing Application	Initial-Access

Sources

Source	URL	Tier
ICS Advisories	https://www.cisa.gov/news-events/ics-advisories/icsa-26-169-03	T1
	https://www.securityweek.com/rockwell-automation-patches-vulnerabil...	T3
	https://www.automation.com/article/rockwell-automation-adds-histori...	T3
CVE-2025-44019 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2025-44019	T1
CVE-2025-44019 - Red Hat Customer Portal	https://access.redhat.com/security/cve/cve-2025-44019	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2025-13036, CVE-2025-44019, CV...	T1

Generated 2026-06-18 14:16 UTC by TJS Security Command Center