INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-30 14:09 UTC

ABB IEC 61850 MMS Stack Denial-of-Service Vulnerabilities Affect Critical Infrastructure Automation Platforms

CVE VULNERABILITY | HIGH | CVSS 7.5

SCC Item ID	SCC-CVE-2026-0105
Type	CVE Vulnerability
Severity	HIGH
CVSS Base Score	7.5
Affected Products	ABB System 800xA, ABB Symphony Plus (S+ Operations, PM 877); IEC 61850 MMS client applications
Published	2026-04-30T12:00:00+00:00
Discovery Source	Rss:T2 Gov

Executive Summary

ABB has disclosed denial-of-service vulnerabilities in the IEC 61850 MMS communication stack used by System 800xA and Symphony Plus automation platforms, deployed in energy, utilities, and manufacturing environments. A network-adjacent attacker who gains access to the IEC 61850 network segment can disrupt MMS communications, potentially halting automated control of industrial processes. Organizations operating these platforms in flat or poorly segmented OT networks carry the highest operational risk.

Technical Analysis

CISA advisory ICSA-26-120-01 (April 30, 2026) and ABB security bulletins 7PAA020125 and 7PAA001023 disclose denial-of-service weaknesses in the IEC 61850 MMS stack embedded in ABB System 800xA and Symphony Plus (S+ Operations, PM 877). Three CWEs are cited: CWE-119 (Improper Restriction of Operations within Memory Bounds), CWE-125 (Out-of-bounds Read), and CWE-400 (Uncontrolled Resource Consumption). Attack vector is network-adjacent, meaning an attacker must have access to the IEC 61850 network segment; remote-only exploitation is not supported. GOOSE protocol traffic is confirmed unaffected. CVSS base score is 7.5 (High). No CVE identifier was assigned in the CISA advisory; CVE assignment status remains unconfirmed as of the disclosure date. CISA KEV listing is not confirmed. Affected IEC 61850 MMS client applications beyond ABB products may also be impacted depending on shared stack components. Patches and mitigations are detailed in ABB advisories 7PAA020125 and 7PAA001023; operators should consult ABB's security library directly for version-specific remediation paths. A third ABB bulletin (7PAA023732)

addresses third-party component involvement in System 800xA.

Action Checklist

1. Preparation: Immediately verify network segmentation for all IEC 61850 network segments hosting ABB System 800xA and Symphony Plus (S+ Operations, PM 877). Confirm that no unauthorized devices have adjacency to the MMS communication stack. If segmentation is absent or incomplete, implement firewall rules or VLAN isolation to restrict access to the IEC 61850 segment to authorized engineering workstations and historian nodes only.
2. Detection: Review IDS/IPS logs and OT network monitoring tools (e.g., Claroty, Dragos, Nozomi; open-source alternatives such as Suricata or Zeek configured with IEC 61850 protocol rules can also provide this visibility) for anomalous MMS traffic patterns: malformed MMS PDUs, abnormal connection rates to MMS server ports (TCP 102), or unexpected resource consumption spikes on ABB server processes. Check ABB System 800xA and Symphony Plus event logs for communication stack errors or unexpected service restarts correlated with external connection attempts.
3. Eradication: Apply patches and mitigations specified in ABB security bulletins 7PAA020125 and 7PAA001023, and review 7PAA023732 for third-party component remediation applicable to System 800xA. Obtain current patch versions directly from ABB's security library (library.e.abb.com) or through your ABB support contact. Validate patch applicability against your specific product versions before deployment in production OT environments.
4. Recovery: After patching, verify MMS communication stack stability by confirming normal process data exchange between clients and servers on the IEC 61850 segment. Monitor OT network traffic for at least 72 hours post-patch for residual anomalies. Confirm GOOSE traffic continuity, as it was unaffected but should be validated as part of post-change verification.
5. Post-Incident: Conduct a segmentation review for all OT environments running IEC 61850. This vulnerability class (network-adjacent DoS against MMS stack) is credible precisely because many OT deployments run flat networks. Map IEC 61850 exposure across all sites. Update ICS network architecture documentation and verify that OT monitoring tools are configured to alert on MMS traffic anomalies as a standing detection control.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to OT security leadership, site operations management, and (if NERC CIP or equivalent regulatory framework applies) compliance officers if active MMS communication disruption is detected on any IEC 61850 segment hosting ABB System 800xA or Symphony Plus, if network scanning reveals TCP 102 is reachable from IT or untrusted network segments, or if patching cannot be completed within the vendor-recommended timeframe and no compensating network isolation is achievable.

Recovery Notes	After applying ABB patches per bulletins 7PAA020125 and 7PAA001023, confirm the ABB System 800xA or Symphony Plus MMS communication stack restarts cleanly and re-establishes normal MMS Associate sessions with all IEC 61850 clients, verifiable via Wireshark TCP 102 capture or ABB OPC diagnostics within the first 10 minutes of service restart. Conduct a parallel GOOSE multicast continuity check using Wireshark EtherType 0x88B8 filter to confirm protection relay and interlock signaling is intact, even though GOOSE was not directly affected by this vulnerability. Maintain elevated network monitoring on the IEC 61850 segment for a minimum of 72 hours post-patch, with alerts tuned to flag any recurrence of malformed MMS PDUs or abnormal TCP 102 connection rates from previously unseen source IPs.
Forensic Artifacts	ABB System 800xA and Symphony Plus Windows Event Logs (Application and System channels) on MMS server nodes, specifically capturing ABB communication stack service fault events, unexpected restarts, and access violation errors timestamped against external connection attempts on TCP 102 — exported via wevtutil to .evtx files before any patching or service restarts. | Full packet capture (pcapng) of TCP port 102 traffic on the IEC 61850 network segment spanning the period of suspected or confirmed DoS activity, preserving malformed MMS PDU structures, abnormal connection rates, and source IP addresses of any non-authorized MMS clients — this is the primary network forensic artifact for identifying the attack source and confirming exploitation of the MMS stack vulnerability. | ABB System 800xA internal diagnostic and trace logs at %ProgramData%\ABB\800xA\Logs\ (or equivalent path per installed version) containing MMS stack error codes and stack trace entries generated when the vulnerable component processed malformed PDUs — these logs may directly correlate with the specific vulnerability mechanism described in bulletins 7PAA020125 and 7PAA001023. | Pre-patch registry export of HKLM\SOFTWARE\ABB\ hive and SHA-256 hashes of ABB MMS stack binaries in the System 800xA or Symphony Plus installation directories, establishing which vulnerable software version was running at the time of the incident and supporting root cause documentation. | Network switch ARP tables and VLAN membership exports from all switches on the IEC 61850 segment, collected immediately upon incident detection, documenting every device that had network adjacency to the ABB MMS stack — critical for determining whether any unauthorized device exploited the flat-network exposure condition described in the advisory.

Per-Action IR Details

Containment — Immediately verify network segmentation for all IEC 61850 network segments hosting ABB System 800xA and Symphony Plus (S+ Operations, PM 877). Confirm that no unauthorized devices have adjacency to the MMS communication stack. If segmentation is absent or incomplete, implement firewall rules or VLAN isolation to restrict access to the IEC 61850 segment to authorized engineering workstations and historian nodes only.

NIST Phase: Containment

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

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

Compensating: On a 2-person team without managed firewalls: use Windows Firewall with Advanced Security (wf.msc) on ABB System 800xA server nodes to block inbound TCP 102 (MMS/TPKT) from all sources except the specific IP addresses of authorized engineering workstations and historian nodes — command: `netsh advfirewall firewall add rule name='Block-MMS-Unauthorized' protocol=TCP dir=in localport=102 action=block`. On network switches, apply port-based VLAN isolation using the switch CLI to move unauthorized or unidentified devices off the IEC 61850 VLAN. Use Wireshark on a span port to enumerate all devices currently communicating on TCP 102 before locking down rules.

Evidence: Before changing any firewall rules or VLAN assignments, capture a full packet capture of the IEC 61850 network segment using Wireshark or tcpdump, filtering on TCP port 102, to establish a baseline of all current MMS client-server sessions and document any anomalous source IPs sending malformed MMS PDUs. Export the ARP table from all switches on the IEC 61850 VLAN (`show arp` or `arp -a` on Windows) to record all MAC-to-IP mappings — this documents which devices had adjacency to the MMS stack prior to containment and is critical evidence if a DoS event has already occurred.

Detection — Review IDS/IPS logs and OT network monitoring tools (e.g., Claroty, Dragos, Nozomi) for anomalous MMS traffic patterns: malformed MMS PDUs, abnormal connection rates to MMS server ports (TCP 102), or unexpected resource consumption spikes on ABB server processes. Check ABB System 800xA and Symphony Plus event logs for communication stack errors or unexpected service restarts correlated with external connection attempts.

NIST Phase: Detection Analysis

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

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

Compensating: Without Claroty/Dragos/Nozomi: deploy Zeek (formerly Bro) with the IEC 61850/MMS protocol analyzer on a Linux host connected to a span port on the IEC 61850 switch to parse and log MMS PDU structure, connection rates, and protocol anomalies to JSON logs in `/opt/zeek/logs/current/`. On ABB System 800xA nodes, run `Get-EventLog -LogName System -Source '*ABB*' -Newest 500 | Where-Object {$_.EntryType -eq 'Error' -or $_.EntryType -eq 'Warning'}` in PowerShell to extract service crash or restart events from the 800xA communication stack. For Symphony Plus PM 877 nodes, review the Windows Event Log Application channel filtering on Source 'SymphonyPlus' or 'AC800M' for stack fault events. Use Wireshark with display filter `mms` (requires MMS dissector) to manually identify malformed PDUs.

Evidence: Collect and preserve: (1) ABB System 800xA node Application and System Windows Event Logs, specifically events indicating ABB OPC server or MMS communication stack service faults, restarts, or access violations — export via `wevtutil epl Application C:\IR\800xA_App.evtx` and `wevtutil epl System C:\IR\800xA_Sys.evtx`; (2) Zeek or span-port packet capture logs showing source IPs, connection timestamps, and PDU sizes for all TCP 102 sessions in the window preceding any detected process disruption; (3) ABB System 800xA internal diagnostic logs located at `%ProgramData%\ABB\800xA\Logs\` (path may vary by version — confirm with ABB bulletin 7PAA020125) for stack error codes tied to malformed MMS PDU processing.

Eradication — Apply patches and mitigations specified in ABB security bulletins 7PAA020125 and 7PAA001023, and review 7PAA023732 for third-party component remediation applicable to System 800xA. Obtain current patch versions directly from ABB's security library (library.e.abb.com) or through your ABB support contact. Validate patch applicability against your specific product versions before deployment in production OT environments.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CM-3 (Configuration Change Control), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Without an automated patch management platform: manually download patches from `library.e.abb.com` using an air-gapped USB transfer process — hash each downloaded patch installer with `Get-FileHash -Algorithm SHA256 ` in PowerShell and compare against the hash published in ABB bulletins 7PAA020125 and 7PAA001023 before transfer to the OT environment. Test patch installation on a staging or non-production 800xA node (or Symphony Plus lab instance) first; document MMS stack service version pre- and post-patch using `sc query ` and ABB's own version query tools. Take a VM snapshot or full disk image of production nodes prior to patching as a rollback point.

Evidence: Before applying ABB patches, collect: (1) current installed software version strings for ABB System 800xA and Symphony Plus S+ Operations/PM 877 components via `HKLM\SOFTWARE\ABB\` registry hive export (`reg

export HKLM\SOFTWARE\ABB C:\IR\ABB_registry_precheck.reg`) to establish pre-patch baseline; (2) SHA-256 hashes of the existing ABB MMS stack DLLs or binaries in the 800xA installation directory (typically `C:\Program Files (x86)\ABB\...`) using `Get-FileHash` — these hashes confirm which vulnerable version was running if the incident requires post-hoc analysis; (3) a system process list snapshot (`Get-Process | Export-Csv C:\IR\processes_precheck.csv`) to record ABB service states before any changes are made.

Recovery — After patching, verify MMS communication stack stability by confirming normal process data exchange between clients and servers on the IEC 61850 segment. Monitor OT network traffic for at least 72 hours post-patch for residual anomalies. Confirm GOOSE traffic continuity, as it was unaffected but should be validated as part of post-change verification.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST SI-6 (Security and Privacy Function Verification), NIST CP-10 (System Recovery and Reconstitution), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Without an OT-aware network monitor: run Wireshark on a span port for 72 hours with a dual capture filter — `tcp.port == 102` for MMS sessions and `eth.type == 0x88b8` for GOOSE frames (IEC 61850 GOOSE uses EtherType 0x88B8 over Ethernet multicast, not TCP) — to simultaneously confirm MMS client-server session re-establishment and GOOSE multicast continuity. Use ABB System 800xA's built-in OPC diagnostics or the 800xA System Status Display to confirm process data is flowing from field devices through the MMS stack to operator displays. Log all post-patch MMS session establishment events at 15-minute intervals for the 72-hour window using a scheduled PowerShell script that queries ABB service status and writes to a CSV.

Evidence: During recovery verification, preserve: (1) a Wireshark capture file (`.pcapng`) spanning the first 30 minutes post-patch restart showing successful MMS Associate/Conclude handshakes between IEC 61850 clients and the ABB MMS server — this confirms the patched stack is handling connection establishment correctly; (2) ABB System 800xA event logs post-patch showing clean communication stack startup without fault codes, captured via `wevtutil epl Application C:\IR\800xA_App_postpatch.evtx`; (3) a timestamped screenshot or export of the 800xA System Status Display or Symphony Plus Operations console showing process data values updating normally from IEC 61850-connected field devices within the first 10 minutes of stack restart.

Post-Incident — Conduct a segmentation review for all OT environments running IEC 61850. This vulnerability class (network-adjacent DoS against MMS stack) is credible precisely because many OT deployments run flat networks. Map IEC 61850 exposure across all sites. Update ICS network architecture documentation and verify that OT monitoring tools are configured to alert on MMS traffic anomalies as a standing detection control.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), NIST CA-7 (Continuous Monitoring), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Without enterprise asset management tools: build an IEC 61850 exposure map using active network scanning with `nmap -p 102 --open -sV ` run from an authorized engineering workstation on each OT subnet to enumerate all hosts responding on TCP 102 (MMS). Document results in a spreadsheet mapping each MMS server IP to its ABB product (800xA node, Symphony Plus S+ Operations server, or PM 877 controller), firmware version, and network segment. For standing MMS anomaly detection without a commercial OT monitor, create a Zeek or Snort/Suricata rule alerting on TCP 102 connection rates exceeding a threshold (e.g., >10 new connections per minute from a single source) or on TCP 102 sessions with abnormally small or malformed initial PDU sizes indicative of the exploit pattern described in ABB bulletins 7PAA020125 and 7PAA001023.

Evidence: For the lessons-learned record and updated architecture documentation, collect: (1) the complete pre-remediation network topology diagram or switch VLAN configuration exports showing which IEC 61850 segments lacked isolation — these document the flat-network risk condition that made this vulnerability exploitable; (2) the full asset inventory output from the nmap TCP 102 scan across all sites, preserved as a dated CSV, establishing the IEC

61850 attack surface baseline for future vulnerability assessments; (3) a written record of which ABB product versions were running at each site prior to patching, sourced from the registry exports collected during eradication, to support future disclosure obligations or lessons-learned reporting under NERC CIP or ICS-CERT voluntary reporting if applicable.

Detection Guidance

Primary detection surface is OT network traffic monitoring. Look for: (1) Anomalous or malformed MMS PDUs on TCP port 102 directed at ABB System 800xA or Symphony Plus nodes; unexpected packet sizes or malformed ISO COTP/MMS headers may indicate exploitation attempts triggering CWE-125 or CWE-119 conditions. (2) Elevated connection rates or resource exhaustion patterns on MMS server processes, consistent with CWE-400 exploitation; monitor CPU and memory utilization on affected ABB servers. (3) Unexpected process or service restarts on System 800xA or Symphony Plus nodes correlated with inbound IEC 61850 network activity. (4) ABB system event logs showing MMS communication stack errors, stack faults, or service unavailability events. OT-specific NDR tools (Dragos Platform, Claroty, Nozomi Networks Guardian) with IEC 61850 protocol awareness are the most effective detection layer. As of the disclosure date, no public IOCs have been published in threat intelligence feeds; monitor ABB advisories and CISA ICS-CERT updates for indicators as exploitation activity emerges.

Framework Mappings

MITRE-ATTACK

- **T0869** — Standard Application Layer Protocol
- **T0816** — Device Restart/Shutdown
- **T0835** — Manipulate I/O Image
- **T0827** — Loss of Control
- **T0886** — Remote Services
- **T1499** — Endpoint Denial of Service
- **T0814** — Denial of Service
- **T0855** — Unauthorized Command Message

NIST-800-53R5

- **SC-5** — Denial-of-Service Protection
- **SI-16** — Memory Protection
- **SI-10** — Information Input Validation

CIS-V8

- **13.8** — Deploy a Network Intrusion Prevention Solution
- **16.10** — Apply Secure Design Principles in Application Architectures

OWASP-TOP10-2021

- **A03:2021** — Injection

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T0869	Standard Application Layer Protocol	Command-And-Control
T0816	Device Restart/Shutdown	Inhibit-Response-Function
T0835	Manipulate I/O Image	Inhibit-Response-Function
T0827	Loss of Control	Impact
T0886	Remote Services	Initial-Access
T1499	Endpoint Denial of Service	Impact
T0814	Denial of Service	Inhibit-Response-Function
T0855	Unauthorized Command Message	Impair-Process-Control

Sources

Source	URL	Tier
ICS Advisories	https://www.cisa.gov/news-events/ics-advisories/icsa-26-120-01	T1
[PDF] Denial of Service Vulnerabilities in System 800xA, Symphony® Plus ...	https://library.e.abb.com/public/8f5dcf14a3b342048f0c7daf8b0374d7/7...	T3
[PDF] Denial of Service Vulnerabilities in System 800xA, Symphony® Plus ...	https://library.e.abb.com/public/6ceab2e7a3144aae9098b90a55c4d0e8/7...	T3
[PDF] System 800xA affected by 3rd party component vulnerabilities - ABB	https://search.abb.com/library/Download.aspx?DocumentID=7PAA023732&...	T3
[Control systems] ABB security advisory (AV26-346) - Cyber.gc.ca	https://www.cyber.gc.ca/en/alerts-advisories/control-systems-abb-se...	T3

Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-04-30 14:09 UTC by TJS Security Command Center