INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-19 14:34 UTC

# No Patch Coming: Mitsubishi Electric FX5-ENET/IP Ethernet Module Permanently Exposed to Remote DoS

**CVE VULNERABILITY** | **HIGH** | CVSS 7.5

| | |
|---|---|
| **SCC Item ID** | SCC-CVE-2026-0337 |
| **Type** | CVE Vulnerability |
| **CVE ID** | CVE-2026-8806 |
| **Severity** | HIGH |
| **CVSS Base Score** | 7.5 |
| **Affected Products** | Mitsubishi Electric MELSEC iQ-F Series FX5-ENET/IP Ethernet Module (all versions) |
| **Published** | 2026-06-18T12:00:00+00:00 |
| **Discovery Source** | Rss:T2 Gov |

## Executive Summary

A remotely exploitable denial-of-service vulnerability affects all versions of the Mitsubishi Electric MELSEC iQ-F Series FX5-ENET/IP Ethernet Module, a component commonly deployed in critical manufacturing and industrial control environments. Mitsubishi Electric has confirmed no patch will be issued, making this a permanent, unresolvable vulnerability that requires compensating controls to manage. Organizations operating this module in production OT/ICS environments face ongoing risk of remote service disruption with no vendor-provided remediation path.

## Technical Analysis

CVE-2026-8806 (CVSS 8.7 HIGH per CISA advisory ICSA-26-169-06) affects all versions of the Mitsubishi Electric MELSEC iQ-F Series FX5-ENET/IP Ethernet Module. The vulnerability is rooted in CWE-440 (Expected Behavior Violation) and CWE-400 (Uncontrolled Resource Consumption), meaning a remote, unauthenticated attacker can send crafted network traffic to exhaust module resources and cause a denial-of-service condition, disrupting Ethernet/IP communications to the affected PLC. No authentication is required. MITRE ATT&CK for ICS techniques mapped include T0884 (Connection Proxy), T0816 (Device Restart/Shutdown), T1498 (Network Denial of Service), T0814 (Denial of Control), and T1499 (Endpoint Denial of Service). Mitsubishi Electric has confirmed no patch will be released for any version of this product. Permanent mitigations are limited to network isolation and access control filtering per the CISA advisory. Note: source verification is required to confirm the correct CVE ID (CVE-2026-8806 vs. CVE-2026-28806 in NVD reference) before operational action.

## Action Checklist

1. Step 1: Containment. Immediately isolate all MELSEC iQ-F Series FX5-ENET/IP Ethernet Modules from untrusted network segments. Place affected modules behind a firewall or industrial demilitarized zone (DMZ) that blocks inbound EtherNet/IP traffic (TCP/UDP port 44818) from any host not explicitly authorized. Reference CISA advisory ICSA-26-169-06 for Mitsubishi Electric's specific network isolation guidance and confirm the correct service ports for your module configuration.
2. Step 2: Detection. Audit your asset inventory (CIS 1.1) to identify all deployed FX5-ENET/IP modules. Review network flow logs and IDS/IPS alerts for unexpected high-volume or malformed EtherNet/IP traffic to module IP addresses. Enable logging on network boundary devices per NIST AU-2 and collect those logs per CIS 8.2. Anomalous connection volume or repeated TCP resets to EtherNet/IP ports from external or untrusted hosts are behavioral indicators of exploitation attempts.
3. Step 3: Eradication. No patch exists and none will be issued. The only eradication path is permanent compensating control: enforce strict access control lists (ACLs) permitting EtherNet/IP communications only from explicitly authorized engineering workstations and PLCs (NIST SC-1 principle of least privilege; CIS 3.3). Disable remote access to the module from any network segment not operationally required. Document exceptions per your organization's risk acceptance process.
4. Step 4: Recovery. After implementing network isolation, verify module responsiveness from authorized hosts only. Confirm ACL rules are enforced at the network layer and validate no unauthorized hosts can reach EtherNet/IP service ports. Monitor module availability continuously; configure alerts for unexpected communication failures per NIST AU-5. Log all access attempts per NIST AU-12 and retain logs per NIST AU-11 to support post-event analysis.
5. Step 5: Post-Incident. Review your OT/ICS asset inventory (CIS 1.1) for other end-of-support or no-patch-available devices operating in network-exposed positions. This vulnerability exposes a control gap in lifecycle management: Mitsubishi Electric has confirmed no remediation path, which means continued operation depends entirely on compensating controls. Update your risk register to reflect this as a permanent residual risk. Develop or update your ICS incident response plan per NIST IR-8 to include scenarios where vendor remediation is unavailable.

## IR / Forensic Enrichment

| | |
|---|---|
| **Triage Priority** | IMMEDIATE |
| **Escalation Criteria** | Escalate to OT security leadership and plant/operations management immediately if network monitoring detects repeated EtherNet/IP connection attempts to FX5-ENET/IP module IPs from unauthorized hosts, if the module becomes unresponsive during production operations indicating a successful DoS, or if the organization lacks the network segmentation capability to implement compensating controls — as continued operation without isolation constitutes unacceptable residual risk under a permanent no-patch vulnerability in a critical manufacturing environment. |

| | |
|---|---|
| **Recovery Notes** | Because CVE-2026-8806 has no vendor patch and affects all firmware versions of the FX5-ENET/IP module, recovery is not a return to pre-incident state but a transition to a permanently compensating-control-dependent operational posture. After ACL enforcement, validate module availability from authorized engineering workstations daily for the first two weeks using GX Works3 connection tests, then shift to automated 5-minute polling via cron or equivalent. Monitor firewall deny logs for ports 44818 and 2222 continuously for 90 days post-containment to detect any reconnaissance or exploitation attempt pattern that suggests an adversary was already aware of the exposure before controls were applied. |
| **Forensic Artifacts** | Firewall and managed switch deny logs for TCP/UDP port 44818 and port 2222 destined to FX5-ENET/IP module IP addresses — malformed or high-volume EtherNet/IP CIP connection attempts from unauthorized source IPs are the primary indicator of CVE-2026-8806 exploitation attempts against this specific module. \| Wireshark/tcpdump pcap files captured on the OT network segment hosting the FX5-ENET/IP module, filtered on the module IP and EtherNet/IP ports, preserving packet timing and payload structure to identify CIP protocol anomalies or flood patterns consistent with the remote DoS mechanism. \| NetFlow or sFlow records from the boundary router or aggregation switch covering the FX5-ENET/IP module subnet — elevated bytes-per-second or connection-per-second metrics to the module IP on port 44818 without corresponding authorized source IPs indicate active or attempted exploitation. \| ARP and MAC address table exports from the OT network switch (`show arp`, `show mac address-table`) timestamped at the time of detection — unexpected source MACs communicating with the module IP may indicate a laterally-moved attacker or rogue device attempting to reach the vulnerable service. \| Module availability and communication logs from the Mitsubishi Electric GX Works3 engineering environment, specifically connection error records and timeout events correlated against the network anomaly timestamps, which would confirm whether a DoS condition was successfully induced on the FX5-ENET/IP module during the exposure window. |

### Per-Action IR Details

**Step 1: Containment — Immediately isolate all MELSEC iQ-F Series FX5-ENET/IP Ethernet Modules from untrusted network segments. Place affected modules behind a firewall or industrial demilitarized zone (DMZ) that blocks inbound EtherNet/IP traffic (TCP/UDP port 44818 and port 2222) from any host not explicitly authorized. Reference CISA advisory ICSA-26-169-06 for Mitsubishi Electric's specific network isolation guidance.**

**NIST Phase:** Containment

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

**Controls:** CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

**Compensating:** On a Linux-based perimeter device or OT firewall (pfSense, iptables), immediately apply: `iptables -I FORWARD -p tcp --dport 44818 ! -s -j DROP` and `iptables -I FORWARD -p udp --dport 44818 ! -s -j DROP`, mirroring both rules for port 2222. If the module sits behind a managed switch with ACL capability, push port-based ACLs from the CLI blocking EtherNet/IP ports to the module's IP from all VLANs except the authorized PLC/HMI VLAN. Verify with a Wireshark capture on the DMZ interface confirming no EtherNet/IP SYN packets from unauthorized hosts reach the module IP.

**Evidence:** Before activating firewall rules or reconfiguring switch ACLs, capture active network state to document any in-progress exploitation: run `netstat -an | grep -E '44818|2222'` or `ss -tnup sport = :44818` on any Linux host with visibility to the module subnet to record active connection table entries; capture a short Wireshark pcap (minimum 5 minutes) on the network segment hosting the FX5-ENET/IP module, filtered on `tcp.port == 44818 or udp.port == 44818 or tcp.port == 2222`, preserving source IPs and packet timing that would indicate a DoS flood or malformed CIP packet sequence; export NetFlow or sFlow records from the boundary router or managed switch covering at least the

prior 24 hours before rule changes alter traffic baselines.

**Step 2: Detection — Audit your asset inventory (CIS 1.1) to identify all deployed FX5-ENET/IP modules. Review network flow logs and IDS/IPS alerts for unexpected high-volume or malformed EtherNet/IP traffic to module IP addresses. Enable logging on network boundary devices per NIST AU-2 and collect those logs per CIS 8.2. Anomalous connection volume or repeated TCP resets to EtherNet/IP ports from external or untrusted hosts are behavioral indicators of exploitation attempts.**

**NIST Phase:** Detection Analysis

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

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

**Compensating:** Use `nmap -sV -p 44818,2222 ` to enumerate all hosts responding on EtherNet/IP ports and cross-reference against your asset inventory to identify undocumented FX5-ENET/IP modules. For traffic anomaly detection without a SIEM, configure a Snort or Suricata rule targeting malformed CIP (Common Industrial Protocol) packets to the module IP: `alert tcp any any -> 44818 (msg:"Malformed CIP to FX5-ENET/IP"; flags:S; threshold: type both, track by_src, count 20, seconds 10; sid:9000001; rev:1;)`. Export and manually grep firewall or switch syslog for repeated TCP RST sequences: `grep -E 'RST|REJECT' /var/log/firewall.log | grep '44818' | awk '{print $1,$5}' | sort | uniq -c | sort -rn`.

**Evidence:** No host-altering actions occur in this step, but preserve the following before any subsequent containment action modifies live state: export the full ARP table from the OT network switch (`show arp` via CLI) to record module MAC-to-IP bindings before network changes; pull the existing firewall or IDS/IPS alert history covering TCP/UDP port 44818 and port 2222 to the FX5-ENET/IP module IPs for at least 30 days prior, noting timestamps and source IPs of any high-volume or repeated connection attempts; if the module exposes a web interface or diagnostic page, take a screenshot of its status/health display before any network isolation that would render it unreachable.

**Step 3: Eradication — No patch exists and none will be issued. The only eradication path is permanent compensating control: enforce strict access control lists (ACLs) permitting EtherNet/IP communications only from explicitly authorized engineering workstations and PLCs (NIST SC-1 principle of least privilege; CIS 3.3). Disable remote access to the module from any network segment not operationally required. Document exceptions per your organization's risk acceptance process.**

**NIST Phase:** Eradication

**Reference:** NIST 800-61r3 §3.4 — Eradication

**Controls:** CIS 3.3 (Configure Data Access Control Lists), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

**Compensating:** Because no vendor patch exists for CVE-2026-8806, eradication is achieved entirely through network-layer ACL enforcement. On a Cisco or similar managed switch, apply: `ip access-list extended FX5-ENET-PERMIT / permit tcp host eq 44818 / permit tcp host eq 44818 / deny tcp any host eq 44818 log / deny udp any host eq 44818 log`. Document each authorized source IP in a plain-text exception register with business justification and reviewer sign-off, stored outside the OT environment. Verify ACL effectiveness using `nmap -p 44818,2222 ` from an unauthorized host — the port must appear filtered, not open.

**Evidence:** Before finalizing ACL changes that permanently restrict communications to the module, capture: a Wireshark pcap from the authorized engineering workstation confirming normal CIP session establishment to the FX5-ENET/IP module (to establish a baseline for post-control validation); the current module configuration backup if accessible via GX Works3 or the Mitsubishi Electric engineering tool, preserving the pre-isolation operational state; and the full switch ACL configuration before modification (`show running-config | include access-list`) as a change-control baseline artifact.

**Step 4: Recovery — After implementing network isolation, verify module responsiveness from authorized hosts only. Confirm ACL rules are enforced at the network layer and validate no unauthorized hosts can reach EtherNet/IP service ports. Monitor module availability continuously; configure alerts for unexpected**

**communication failures per NIST AU-5. Log all access attempts per NIST AU-12 and retain logs per NIST AU-11 to support post-event analysis.**

**NIST Phase:** Recovery

**Reference:** NIST 800-61r3 §3.5 — Recovery

**Controls:** NIST AU-5 (Response To Audit Logging Process Failures), NIST AU-12 (Audit Record Generation), NIST AU-11 (Audit Record Retention), NIST AU-4 (Audit Storage Capacity)

**Compensating:** Validate module availability from authorized engineering workstations using the Mitsubishi Electric GX Works3 ping/connection test or a raw EtherNet/IP CIP identity request: `python3 -c "import socket; s=socket.socket(); s.connect(('',44818)); print('reachable'); s.close()"`. For continuous availability monitoring without enterprise tooling, configure a cron job on a Linux host in the authorized VLAN: `*/5 * * * * nc -z -w3 44818 || echo "FX5-ENET/IP UNREACHABLE $(date)" >> /var/log/fx5_monitor.log` and alert on log entries. Retain firewall deny logs with timestamps for a minimum of 90 days to support post-event reconstruction of any exploitation attempt pattern.

**Evidence:** Recovery validation is non-destructive, but capture the following as post-control baseline artifacts: a Wireshark pcap from the authorized engineering VLAN confirming clean CIP session establishment to the FX5-ENET/IP module after ACL enforcement, which documents restored normal operational state; a current export of all firewall and switch ACL deny log entries for ports 44818 and 2222 to preserve evidence of any exploitation attempts that occurred during the exposure window before containment; and a timestamped screenshot or log export from GX Works3 confirming the module is responsive and in expected operational mode, establishing a clean-state benchmark for future anomaly comparison.

**Step 5: Post-Incident — Review your OT/ICS asset inventory (CIS 1.1) for other end-of-support or no-patch-available devices operating in network-exposed positions. This vulnerability exposes a control gap in lifecycle management: Mitsubishi Electric has confirmed no remediation path, which means continued operation depends entirely on compensating controls. Update your risk register to reflect this as a permanent residual risk. Develop or update your ICS incident response plan per NIST IR-8 to include scenarios where vendor remediation is unavailable.**

**NIST Phase:** Post Incident

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

**Controls:** CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), NIST IR-8 (Incident Response Plan), NIST IR-5 (Incident Monitoring)

**Compensating:** Conduct a tabletop exercise specifically scoped to the CVE-2026-8806 no-patch scenario: walk through what happens if the FX5-ENET/IP module is successfully taken offline during a production shift, who is notified, what the manual fallback process is, and how long operations can sustain without the affected module. Use a plain spreadsheet risk register with columns for Asset, CVE, CVSS, Vendor Patch Status (mark CVE-2026-8806 as 'Permanent/No Fix'), Compensating Control Owner, and Review Date (quarterly). Cross-reference the OT asset inventory against the CISA Known Exploited Vulnerabilities catalog and Mitsubishi Electric's published advisories semi-annually to catch any additional end-of-support disclosures.

**Evidence:** No live-state alteration occurs in this phase; preserve the following for lessons-learned documentation: the complete incident timeline from initial detection through containment and recovery, including all firewall log exports and pcaps collected during earlier phases, retained per NIST AU-11 for a minimum of 90 days or per your organization's OT incident record retention policy; the final ACL configuration as applied to all network devices protecting the FX5-ENET/IP module, archived as a configuration management artifact under change control; and the updated risk register entry for CVE-2026-8806 documenting CVSS 7.5 severity, permanent no-patch status per Mitsubishi Electric's confirmation, compensating controls implemented, residual risk acceptance, and the name and date of the authorizing risk owner.

## Detection Guidance

Monitor network flows destined for all deployed FX5-ENET/IP module IP addresses, specifically on EtherNet/IP service ports (TCP/UDP 44818). Indicators of exploitation include abnormally high connection rates, malformed EtherNet/IP frames, or repeated connection attempts from hosts outside the authorized engineering network. Enable logging on perimeter and OT network firewalls per NIST AU-2 and ensure logs are collected and retained per CIS 8.2 and NIST AU-11. Behavioral indicators include unexpected module unresponsiveness, PLC communication timeouts correlated with external network activity, and resource exhaustion events logged by the module or adjacent network devices. No CVE-specific signatures or IOCs are available from the CISA advisory at this time. Network baseline deviation, specifically traffic volume spikes to EtherNet/IP ports from unauthorized source addresses, is the primary detection signal. Review module access logs and network flow records for unauthorized connection attempts per NIST AU-12.

## Framework Mappings

### MITRE-ATTACK

- **T0884** — Connection Proxy
- **T0816** — Device Restart/Shutdown
- **T1498** — Network Denial of Service
- **T0814** — Denial of Service
- **T1499** — Endpoint Denial of Service

### NIST-800-53R5

- **SC-5** — Denial-of-Service Protection

### CIS-V8

- **13.8** — Deploy a Network Intrusion Prevention Solution
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

### ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

## MITRE ATT&CK Mapping

| Technique ID | Technique Name | Tactic |
|---|---|---|
| T0884 | Connection Proxy | Command-And-Control |
| T0816 | Device Restart/Shutdown | Inhibit-Response-Function |
| T1498 | Network Denial of Service | Impact |
| T0814 | Denial of Service | Inhibit-Response-Function |
| T1499 | Endpoint Denial of Service | Impact |

## Sources

| Source | URL | Tier |
|---|---|---|
| **ICS Advisories** | https://www.cisa.gov/news-events/ics-advisories/icsa-26-169-06 | T1 |
| **CVE-2026-28806 Detail - NVD** | https://nvd.nist.gov/vuln/detail/CVE-2026-28806 | T1 |
| **June 2026 Patch Tuesday: Updates and Analysis \| CrowdStrike** | https://www.crowdstrike.com/en-us/blog/patch-tuesday-analysis-june-... | T3 |
| **April 2026 CVE Landscape - Recorded Future** | https://www.recordedfuture.com/blog/april-cve-landscape | T3 |
| **NVD** | https://nvd.nist.gov/vuln/detail/CVE-2026-8806 | T1 |



Generated 2026-06-19 14:34 UTC by TJS Security Command Center