America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

ICS ADVISORY

Mitsubishi Electric MELSEC iQ-F Series

Release Date: November 19, 2024 **Alert Code:** ICSA-24-324-01

RELATED TOPICS: INDUSTRIAL CONTROL SYSTEM VULNERABILITIES </topics/industrial-control-systems/industrial-control-system-vulnerabilities>, INDUSTRIAL CONTROL SYSTEMS </topics/industrial-control-systems>

View CSAF <https://github.com/cisagov/csaf>

1. EXECUTIVE SUMMARY

- **CVSS v3 7.5**
- **ATTENTION**: Exploitable remotely/low attack complexity
- **Vendor**: Mitsubishi Electric Corporation
- **Equipment**: MELSEC iQ-F Series
- **Vulnerability**: Improper Validation of Specified Type of Input

2. RISK EVALUATION

Successful exploitation of this vulnerability could allow a remote attacker to cause a denial-of-service condition in Ethernet communication on the module. A system reset of the module is required for recovery.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

Mitsubishi Electric reports that the following versions of MELSEC iQ-F Series Ethernet module and EtherNet/IP module are affected:

- MELSEC iQ-F Series FX5-ENET: version 1.100 and later
- MELSEC iQ-F Series FX5-ENET/IP: version 1.100 to 1.104

3.2 Vulnerability Overview

3.2.1 Improper Validation of Specified Type of Input CWE-1287

<https://cwe.mitre.org/data/definitions/1287.html>

A denial-of-service vulnerability due to improper validation of a specified type of input exists in MELSEC iQ-F Ethernet Module and EtherNet/IP Module.

CVE-2024-8403 has been assigned to this vulnerability. A CVSS v3.1 base score of 7.5 has been calculated; the CVSS vector string is (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H <https://www.first.org/cvss/calculator/3.1#cvss:3.1/av:n/ac:l/pr:n/ui:n/s:u/c:n/i:n/a:h>).

3.3 BACKGROUND

- **CRITICAL INFRASTRUCTURE SECTORS:** Critical Manufacturing
- **COUNTRIES/AREAS DEPLOYED:** Worldwide
- **COMPANY HEADQUARTERS LOCATION:** Japan

3.4 RESEARCHER

Mitsubishi Electric reported this vulnerability to CISA.

4. MITIGATIONS

Mitsubishi Electric has fixed this issue in MELSEC iQ-F Series FX5-ENET/IP version 1.106 or later. The firmware update file can be found on Mitsubishi Electric's download page. <https://www.mitsubishielectric.com/fa/download/index.html> Refer to "9 FIRMWARE UPDATE FUNCTION" in the "MELSEC iQ-F FX5 User's Manual (Application)" for information on how to update the firmware.

Mitsubishi Electric recommends that users take the following mitigations/workarounds to minimize the risk of exploiting this vulnerability:

- Use within a LAN and block access from untrusted networks and hosts through firewalls.
- Restrict physical access to the product, as well as to computers and network devices located within the same network as the product.
- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when internet access is required.
- Use IP filter function to block access from untrusted hosts. For details on the IP filter function, please refer to the following manual: MELSEC iQ-F FX5 User's Manual (Communication) "13.1 IP Filter Function"

For specific update instructions and additional details see the Mitsubishi Electric advisory. <https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2024-009_en.pdf>

Please contact your local Mitsubishi Electric representative. <https://www.mitsubishielectric.com/fa/support/index.html>

CISA recommends users take defensive measures to minimize the risk of exploitation of this vulnerability, such as:

- Minimize network exposure for all control system devices and/or systems, ensuring they are not accessible from the internet <https://www.cisa.gov/uscert/ics/alerts/ics-alert-10-301-01>.
- Locate control system networks and remote devices behind firewalls and isolating them from business networks.
- When remote access is required, use more secure methods, such as virtual private networks (VPNs), recognizing VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as the connected devices.

CISA reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

CISA also provides a section for control systems security recommended practices <https://www.cisa.gov/resources-tools/resources/ics-recommended-practices> on the ICS webpage on cisa.gov/ics <https://www.cisa.gov/topics/industrial-control-systems>. Several CISA products detailing cyber defense best practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies <https://us-cert.cisa.gov/sites/default/files/recommended_practices/nccic_ics-cert_defense_in_depth_2016_s508c.pdf>.

CISA encourages organizations to implement recommended cybersecurity strategies for proactive defense of ICS assets <https://www.cisa.gov/sites/default/files/publications/cybersecurity_best_practices_for_industrial_control_systems.pdf>.

Additional mitigation guidance and recommended practices are publicly available on the ICS webpage at cisa.gov/ics <https://www.cisa.gov/topics/industrial-control-systems> in the technical information paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies <https://www.cisa.gov/uscert/ics/tips/ics-tip-12-146-01b>.

Organizations observing suspected malicious activity should follow established internal procedures and report findings to CISA for tracking and correlation against other incidents.

No known public exploitation specifically targeting this vulnerability has been reported to CISA at this time.

5. UPDATE HISTORY

- November 19, 2024: Initial Publication

This product is provided subject to this Notification </notification> and this Privacy & Use </privacy-policy> policy.

Vendor

- Mitsubishi Electric

Tags

Sector: Critical Manufacturing Sector </topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/critical-manufacturing-sector>

Topics: Industrial Control System Vulnerabilities </topics/industrial-control-systems/industrial-control-system-vulnerabilities>, Industrial Control Systems </topics/industrial-control-systems>

Please share your thoughts

We recently updated our anonymous product survey; we welcome your feedback.

Related Advisories

MAR 26, 2026 ■ ICS ADVISORY | ICSA-26-085-01

WAGO GmbH & Co. KG Industrial Managed Switches </news-events/ics-advisories/icsa-26-085-01>

MAR 26, 2026 ■ ICS ADVISORY | ICSA-26-085-02

OpenCode Systems OC Messaging and USSD Gateway </news-events/ics-advisories/icsa-26-085-02>

MAR 26, 2026 ■ ICS ADVISORY | ICSA-26-085-03

PTC Windchill Product Lifecycle Management </news-events/ics-advisories/icsa-26-085-03>

MAR 24, 2026 ■ ICS ADVISORY | ICSA-26-083-02

Schneider Electric EcoStruxure Foxboro DCS </news-events/ics-advisories/icsa-26-083-02>

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Central

1-844-Say-CISA contact@cisa.dhs.gov