America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

ICS ADVISORY

Mitsubishi Electric MELSEC iQ-F Series (Update A)

Last Revised: March 31, 2026 **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/blob/develop/csaf_files/ot/white/2024/icsa-24-324-01.json>

Summary

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

The following versions of Mitsubishi Electric MELSEC iQ-F Series (Update A) are affected:

- MELSEC iQ-F Series FX5-ENET >=1.100|<=1.200 (CVE-2024-8403)

- MELSEC iQ-F Series FX5-ENET/IP >=1.100|<=1.104 (CVE-2024-8403)

CVSS	Vendor	Equipment	Vulnerabilities
v3 7.5	Mitsubishi Electric	Mitsubishi Electric MELSEC iQ-F Series (Update A)	Improper Validation of Specified Type of Input

Background

- **Critical Infrastructure Sectors:** Critical Manufacturing
- **Countries/Areas Deployed:** Worldwide
- **Company Headquarters Location:** Japan

Vulnerabilities

Expand All +

CVE-2024-8403 +

Acknowledgments

- Mitsubishi Electric reported this vulnerability to CISA

Legal Notice

All information products included in https://us-cert.cisa.gov/ics are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see https://us-cert.cisa.gov/tlp/.

Recommended Practices

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. 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 on the ICS webpage on cisa.gov/ics. 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.

CISA encourages organizations to implement recommended cybersecurity strategies for proactive defense of ICS assets.

Additional mitigation guidance and recommended practices are publicly available on the ICS webpage at cisa.gov/ics in the technical information paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies.

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.

Revision History

- **Initial Release Date:** 2024-11-19

Date	Revision	Summary
2024-11-19	1	Initial Publication
2026-03-31	2	Update A - Revised version "FX5-ENET".

Legal Notice and Terms of Use

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

APR 30, 2026 ■ ICS ADVISORY | ICSA-26-120-02

APR 30, 2026 ■ ICS ADVISORY | ICSA-26-120-04

[ABB PCM600 </news-events/ics-advisories/icsa-26-120-02>]

[ABB Ability OPTIMAX </news-events/ics-advisories/icsa-26-120-04>]

APR 30, 2026 ■ ICS ADVISORY | ICSA-26-120-03

[ABB Edgenius Management Portal </news-events/ics-advisories/icsa-26-120-03>]

APR 30, 2026 ■ ICS ADVISORY | ICSA-26-120-01

[ABB System 800xA, Symphony Plus IEC 61850 </news-events/ics-advisories/icsa-26-120-01>]

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