America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

ICS ADVISORY

Mitsubishi Electric MELSEC iQ-F Series EtherNet/IP module and Ethernet module

Release Date: March 03, 2026 **Alert Code:** ICSA-26-62-01

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/2026/icsa-26-062-01.json>

Summary

Successful exploitation of these vulnerabilities could allow a remote attacker to cause a denial-of-service condition by continuously sending UDP packets to the affected products.

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

- MELSEC iQ-F Series FX5-ENET/IP Ethernet Module FX5-ENET/IP <=1.106, vers:all/* (CVE-2026-1874, CVE-2026-1876)
- MELSEC iQ-F Series FX5-EIP EtherNet/IP Module FX5-EIP vers:all/* (CVE-2026-1874, CVE-2026-1875)

CVSS	Vendor	Equipment	Vulnerabilities
v3 7.5	Mitsubishi Electric	Mitsubishi Electric MELSEC iQ-F Series EtherNet/IP module and Ethernet module	Always-Incorrect Control Flow Implementation, Improper Resource Shutdown or Release

Background

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

Vulnerabilities

Expand All +

CVE-2026-1874 +

CVE-2026-1875 +

CVE-2026-1876 +

Acknowledgments

- Mitsubishi Electric reported these vulnerabilities to CISA

Legal Notice and Terms of Use

Recommended Practices

CISA recommends users take defensive measures to minimize the risk of exploitation of these vulnerabilities. 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. 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 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.

Advisory Conversion Disclaimer

This ICSA is a republication of Mitsubishi Electric security advisory "2025-021 Multiple denial-of-service vulnerabilities in Ethernet function of MELSEC iQ-F Series EtherNet/IP module and Ethernet module" from a direct conversion of the vendor's Common Security Advisory Framework (CSAF) advisory. This is republished to CISA's website as a means of increasing visibility and is provided "as-is" for informational purposes only. CISA is not responsible for the editorial or technical accuracy of republished advisories and provides no warranties of any kind regarding any information contained within this advisory. Further, CISA does not endorse any commercial product or service. Please contact CISA directly for any questions regarding this advisory.

Revision History

- **Initial Release Date:** 2026-03-03

Date	Revision	Summary
2026-03-03	1	Initial Publication
2026-03-03	2	Initial CISA Republication of Mitsubishi Electric security advisory 2025-021

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 23, 2026 ■ ICS ADVISORY | ICSA-26-113-06

APR 23, 2026 ■ ICS ADVISORY | ICSA-26-113-04

Intrado 911 Emergency Gateway (EGW) </news-events/ics-advisories/icsa-26-113-06>

SpiceJet Online Booking System </news-events/ics-advisories/icsa-26-113-04>

APR 23, 2026 ■ ICS ADVISORY | ICSA-26-113-02

Carlson Software VASCO-B GNSS Receiver </news-events/ics-advisories/icsa-26-113-02>

APR 23, 2026 ■ ICS ADVISORY | ICSA-26-113-01

Yadea T5 Electric Bicycle </news-events/ics-advisories/icsa-26-113-01>

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