# Denial-of-service (DoS) vulnerability in MELSEC iQ-F Series FX5-ENET/IP Ethernet module

Release date: June 18, 2026
Mitsubishi Electric Corporation

## Overview

A denial-of-service (DoS) vulnerability exists in the MELSEC iQ-F Series FX5-ENET/IP Ethernet module. A remote attacker may be able to cause a denial-of-service (DoS) condition in the affected product by continuously sending a large number of communication packets to the Ethernet port of the product in a short period of time, increasing the processing load of the product, preventing the internal anomaly-detection processing from being performed, and causing the communication function to stop. (CVE-2026-8806)

## CVSS[1]

CVE-2026-8806 CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N Base score 8.7

## Affected products

The following products and versions are affected.

| Series | Product Model | Version |
|---|---|---|
| MELSEC iQ-F Series | FX5-ENET/IP Ethernet Module FX5-ENET/IP | all versions |

## Description

A denial-of-service (DoS) vulnerability due to Expected Behavior Violation (CWE-440[2]) exists in the MELSEC iQ-F Series FX5-ENET/IP Ethernet module.

## Impact

A remote attacker may be able to cause a denial-of-service (DoS) condition in the affected product by continuously sending a large number of communication packets to the Ethernet port of the product in a short period of time, increasing the processing load of the product, preventing the internal anomaly-detection processing from being performed, and causing the communication function to stop.

## Countermeasures for Customers

There are no plans to release a fixed version. Please take the mitigations or workarounds measures described in the “Mitigations / Workarounds” section.

In addition, please consider migrating to the successor model, the FX5-EIP EtherNet/IP Module FX5-EIP.

## Mitigations / Workarounds

Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:

- Use a firewall, virtual private network (VPN), etc. to prevent unauthorized access when internet access is required.
- Use the affected product within a LAN and block access from untrusted networks and hosts through firewalls.
- Use the IP filter function of the affected product to block access from untrusted hosts. For details on the IP filter function, refer to “13.1 IP Filter Function” in the MELSEC iQ-F FX5 User’s Manual (Communication).
  The manual can be downloaded from the following site.
  https://www.mitsubishielectric.com/fa/download/index.html
- Restrict physical access to the affected product, as well as to PCs and network devices to which it is connected.
- Install anti-virus software on PCs that can access the affected product.

## Contact information

Please contact your local Mitsubishi Electric representative.

〈Inquiries | MITSUBISHI ELECTRIC FA〉
https://www.mitsubishielectric.com/fa/service-support/index.html

1 https://www.first.org/cvss/v4-0/specification-document

2 https://cwe.mitre.org/data/definitions/440.html