Denial-of-service (DoS) vulnerability in MELSEC iQ-F Series EtherNet/IP module

Release date: June 18, 2026
Mitsubishi Electric Corporation

Overview

A denial-of-service (DoS) vulnerability exists in the EtherNet/IP function of MELSEC iQ-F Series EtherNet/IP module. A remote attacker may be able to cause a denial-of-service (DoS) condition in the affected product by rapidly establishing a large number of TCP connections to it, resulting in an inconsistency in the product's internal connection management process and triggering improper memory access. (CVE-2026-8805)

CVSS[1]

CVE-2026-8805 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-EIP EtherNet/IP Module FX5-EIP	version 1.000 and prior

【Version check procedure】

MELSEC iQ-F Series FX5-EIP EtherNet/IP Module FX5-EIP

Refer to "Common area (module information)" in "Details of buffer memory addresses (module status G29 to G207)" in "Appendix 4 Buffer Memory" in the MELSEC iQ-F FX5-EIP EtherNet/IP Module User's Manual to check the firmware version of the product.

The manual can be downloaded from the following site.
https://www.mitsubishielectric.com/fa/download/index.html

Description

A denial-of-service (DoS) vulnerability due to Integer Overflow or Wraparound (CWE-190[2]) exists in the EtherNet/IP function of MELSEC iQ-F Series EtherNet/IP module.

Impact

A remote attacker may be able to cause a denial-of-service (DoS) condition in the affected product by rapidly establishing a large number of TCP connections to it, resulting in an inconsistency in the internal connection management process and triggering improper memory access.

Countermeasures for Customers

Please download the update file for the fixed version described in the "Countermeasures for Products" section from the website below and apply it. For the update procedure, refer to "9.2 Update Using the Engineering Tool Updating the firmware for the intelligent function module" in the MELSEC iQ-F FX5 User's Manual (Application).

Website:
https://www.mitsubishielectric.com/fa/download/index.html

Countermeasures for Products

The series, product names, and versions that have been fixed are as follows:

Series	Product Model	Version
MELSEC iQ-F Series	FX5-EIP EtherNet/IP Module FX5-EIP	version 1.001 or later

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

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

2 https://cwe.mitre.org/data/definitions/190.html

"13.1 IP Filter Function" in the MELSEC iQ-F FX5 User's Manual (Communication).
- 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