Multiple denial-of-service (DoS) vulnerabilities in Ethernet function of MELSEC iQ-F Series EtherNet/IP module and Ethernet module

Release date: March 03, 2026
Last update date: April 23, 2026
Mitsubishi Electric Corporation

Overview

Multiple denial-of-service (DoS) vulnerabilities exist in Ethernet function of MELSEC iQ-F Series EtherNet/IP module and Ethernet module. A remote attacker may be able to cause a denial-of-service (DoS) condition in the affected products by continuously sending UDP packets to the products. (CVE-2026-1874, CVE-2026-1875, CVE-2026-1876)

CVSS[1]

CVE-2026-1874 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
CVE-2026-1875 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
CVE-2026-1876 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.

CVE-2026-1874
- MELSEC iQ-F Series FX5-ENET/IP Ethernet Module FX5-ENET/IP versions 1.106 and prior
- MELSEC iQ-F Series FX5-EIP EtherNet/IP Module FX5-EIP versions 1.000 and prior

CVE-2026-1875
- MELSEC iQ-F Series FX5-EIP EtherNet/IP Module FX5-EIP versions 1.000 and prior

CVE-2026-1876
- MELSEC iQ-F Series FX5-ENET/IP Ethernet Module FX5-ENET/IP All versions

【Version check procedure】
MELSEC iQ-F Series FX5-ENET/IP Ethernet Module FX5-ENET/IP
Refer to “Firmware version” in “buffer memory addresses” in “Appendix 4 Buffer Memory Details” in the MELSEC iQ-F FX5-ENET/IP Ethernet Module User's Manual to check the firmware version of the product.

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

Description

The following three denial-of-service (DoS) vulnerabilities exist in Ethernet function of MELSEC iQ-F Series EtherNet/IP module and Ethernet module.

CVE ID	Description of the Vulnerability
CVE-2026-1874	Denial-of-service (DoS) vulnerability due to Always-Incorrect Control Flow Implementation (CWE-670[2])
CVE-2026-1875	Denial-of-service (DoS) vulnerability due to Improper Resource Shutdown or Release (CWE-404[3])
CVE-2026-1876	Denial-of-service (DoS) vulnerability due to Improper Resource Shutdown or Release (CWE-404)

Impact

A remote attacker could cause uncontrolled receive buffer consumption in the affected product by continuously sending UDP packets, resulting in a denial-of-service (DoS) condition. A system reset of the product is required for recovery.

1 https://www.first.org/cvss/v4-0/specification-document
2 https://cwe.mitre.org/data/definitions/670.html
3 https://cwe.mitre.org/data/definitions/404.html

Countermeasures for Customers

CVE-2026-1874
CVE-2026-1875

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).

CVE-2026-1876

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

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:

CVE-2026-1874
・MELSEC iQ-F Series FX5-ENET/IP Ethernet Module　FX5-ENET/IP　versions 1.107 or later
・MELSEC iQ-F Series FX5-EIP EtherNet/IP Module　FX5-EIP　versions 1.001 or later

CVE-2026-1875
・MELSEC iQ-F Series FX5-EIP EtherNet/IP Module　FX5-EIP　versions 1.001 or later

Mitigations/Workarounds

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

- 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).
- 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

Update history

April 23, 2026
- Revised Version in “Affected products”
  FX5-EIP
- Revised the description regarding “Countermeasures for Customers”
  FX5-EIP
- Added a module that have been fixed to "Countermeasures for Products".
  FX5-EIP