Denial-of-Service Vulnerability in Ethernet port on MELSEC iQ-F Ethernet Module and EtherNet/IP Module

Release date:November,19, 2024
Mitsubishi Electric Corporation

Overview

Denial-of-Service (DoS) vulnerability due to improper validation of specified type of input (CWE-1287)[1] exists in MELSEC iQ-F Ethernet Module and EtherNet/IP Module. This vulnerability allows a remote attacker to cause a Denial-of-Service (DoS) condition in Ethernet communication on the module by sending specially crafted SLMP packets. (CVE-2024-8403)

CVSS[2]

CVE-2024-8403 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Base Score:7.5

Affected products

Affected products and firmware versions are below.

Series	Model Name	Version
MELSEC iQ-F Series	FX5-ENET	1.100 and later
	FX5-ENET/IP	1.100 to 1.104

<How to check the version>

・FX5-ENET : Refer to "Appendix 4 Buffer Memory>Details of buffer memory addresses>Firmware version" in the "MELSEC iQ-F FX5 Ethernet Module User's Manual".

・FX5-ENET/IP : Refer to "Appendix 4 Buffer Memory>Details of buffer memory addresses>Firmware version" in the "MELSEC iQ-F FX5 EtherNet/IP Module User's Manual".

Description

Denial-of-Service (DoS) vulnerability due to improper validation of specified type of input (CWE-1287) exists in MELSEC iQ-F Ethernet Module and EtherNet/IP Module.

Impact

This vulnerability allows a remote attacker to cause a Denial-of-Service (DoS) condition in Ethernet communication on the module by sending specially crafted SLMP packets. A system reset of the module is required for recovery.

Countermeasures for Customers

<Customers using the affected versions of FX5-ENET>

Take the following Mitigations / Workarounds.

<Customers using the affected versions of FX5-ENET/IP>

Download a fixed firmware update file described in the next section from the following site and update the firmware.

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

Refer to “9 FIRMWARE UPDATE FUNCTION” in the “MELSEC iQ-F FX5 User's Manual (Application)” for information on how to update the firmware.

Countermeasures for Products

The following modules have been fixed.

Series	Model Name	Version
MELSEC iQ-F Series	FX5-ENET/IP	1.106 or later

Mitigations / Workarounds

Mitsubishi Electric recommends that customers take the following mitigations/workarounds to minimize the risk of exploiting this vulnerability:

- Use within a LAN and block access from untrusted networks and hosts through firewalls.
- Restrict physical access to the product, as well as to computers and network devices located within the same network as the product.
- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when internet access is required.
- Use IP filter function to block access from untrusted hosts. For details on the IP filter function, please refer to the following manual.
  MELSEC iQ-F FX5 User's Manual (Communication) "13.1 IP Filter Function"

[1] https://cwe.mitre.org/data/definitions/1287.html

[2] https://www.first.org/cvss/v3.1/specification-document

Contact information

Please contact your local Mitsubishi Electric representative.
< Inquiries | MITSUBISHI ELECTRIC FA >
https://www.mitsubishielectric.com/fa/support/index.html