Information Disclosure and Denial-of-Service(DoS) Vulnerability in MELSEC iQ-F Series CPU module

Release date: May 29, 2025
Mitsubishi Electric Corporation

Overview

Information disclosure and Denial-of-Service(DoS) vulnerability exists in MELSEC iQ-F series CPU module. This vulnerability allows a remote attacker to read information in the product, to cause a Denial-of-Service (DoS) condition in MELSOFT connection (communication with Mitsubishi Electric FA products such as GX Works3 and GOT), or to stop the operation of the CPU module (causing a DoS condtion on the CPU module), by sending specially crafted packets. (CVE-2025-3755)

CVSS[1]

CVE-2025-3755 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H Base Score 9.1

Affected products

Affected products and firmware versions are below.

Series	Product name	Version
MELSEC iQ-F Series	FX5U-xMy/z x=32,64,80, y=T,R, z=ES,DS,ESS,DSS	All versions
	FX5UC-xMy/z x=32,64,96, y=T, z=D,DSS	All versions
	FX5UC-32MT/DS-TS, FX5UC-32MT/DSS-TS, FX5UC-32MR/DS-TS	All versions
	FX5UJ-xMy/z x=24,40,60, y=T,R, z=ES,DS,ESS,DSS	All versions
	FX5UJ-xMy/ES-A*1 x=24,40,60, y=T,R,	All versions
	FX5S-xMy/z x=30,40,60,80*1, y=T,R, z= ES,DS,ESS,DSS	All versions

*1 : These products are sold in limited regions.

Description

Information disclosure and Denial-of-Service(DoS) vulnerability due to Improper Validation of Specified Index, Position, or Offset in Input(CWE-1285[2]) exists in MELSEC iQ-F series CPU module.

Impact

This vulnerability allows a remote attacker to read information in the product, to cause a Denial-of-Service (DoS) condition in MELSOFT connection, or to stop the operation of the CPU module (causing a DoS condtion on the CPU module), by sending specially crafted packets. The product is needed to reset for recovery.

Countermeasures for Customers

There are no plans to release a fixed version, so please take the following mitigations / workarounds.

Mitigations / Workarounds

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

- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when Internet access is required.
- Use within a LAN and block access from untrusted networks and hosts through firewalls.
- Use IP filter function*2 to block access from untrusted hosts.
- Restrict physical access to the affected products and the LAN that is connected by them.

*2: For details on the IP filter function, please refer to the following manual for each product.
"13.1 IP Filter Function" in the MELSEC iQ-F FX5 User's Manual (Communication)

Please download the manual from the following URL.
https://www.mitsubishielectric.com/fa/download/index.html

[1] https://www.first.org/cvss/v3.1/specification-document
[2] https://cwe.mitre.org/data/definitions/1285.html

Contact information

Please contact your local Mitsubishi Electric representative.

<Inquiries | MITSUBISHI ELECTRIC FA>
https://www.mitsubishielectric.com/fa/support/index.html