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

Release date: August 28, 2025
Mitsubishi Electric Corporation

Overview

Information disclosure, information tampering, and Denial of Service (DoS) vulnerability exists in MELSEC iQ-F series CPU module due to Missing Authentication for Critical Function (CWE-306[1]). Since MODBUS/TCP in the products does not have authentication features, an attacker may be able to read or write the device values of the product. In addition, the attacker may be able to stop the operation of the programs. (CVE-2025-7405)

The product models and firmware versions affected by this vulnerability are listed below.

CVSS[2]

CVE-2025-7405 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L Base Socre:7.3

Affected products

Affected products and firmware versions are below.

Series	Product name	Version
MELSEC iQ-F Series	FX5U-xMT/y, FX5U-xMR/z x=32,64,80, y=ES,DS,ESS,DSS, z=ES,DS	1.060 and later
	FX5UC-xMy/z x=32,64,96, y=T, z=D,DSS	1.060 and later
	FX5UC-32MT/DS-TS, FX5UC-32MT/DSS-TS, FX5UC-32MR/DS-TS	1.060 and later
	FX5UJ-xMT/y, FX5UJ-xMR/z x=24,40,60, y=ES,DS,ESS,DSS, z=ES,DS	All Versions
	FX5UJ-xMy/ES-A*1 x=24,40,60, y=T,R	All Versions
	FX5S-xMT/y, FX5S-xMR/z x=30,40,60,80*1, y=ES,DS,ESS,DSS, z=ES,DS	All Versions

*1 : These products are sold in limited regions

Description

Information disclosure, information tampering, and Denial of Service (DoS) vulnerability exists in MELSEC iQ-F series CPU module due to Missing Authentication for Critical Function (CWE-306).

Impact

An attacker may be able to read or write the device values of the product. In addition, the attacker may be able to stop the operation of the programs.

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

Acknowledgement

Mitsubishi Electric would like to thank Thai Do, Minh Pham, Quan Le and Loc Nguyen of Unit 515, OPSWAT.

[1] https://cwe.mitre.org/data/definitions/306.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