Information Disclosure Vulnerability in MELSEC iQ-F Series CPU module

Release date: August 28, 2025
Mitsubishi Electric Corporation

Overview

Information disclosure vulnerability exists in MELSEC iQ-F series CPU module due to Cleartext Transmission of Sensitive Information (CWE-319[1]). An attacker may be able to obtain credential information by intercepting SLMP communication messages (CVE-2025-7731), and read or write the device values of the product by using the obtained credential information. In addition, the attacker may be able to stop the operations of programs.

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

CVSS[2]

CVE-2025-7731 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N Base Score:7.5

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	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-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 vulnerability exists in MELSEC iQ-F series CPU module due to Cleartext Transmission of Sensitive Information (CWE-319).

Impact

An attacker may be able to obtain credential information by intercepting SLMP communication messages, and read or write the device values of the product by using the obtained credential information. In addition, the attacker may be able to stop the operations of 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 virtual private network (VPN) or similar to encrypt SLMP communication.
- Restrict physical access to the LAN that is connected by the affected products.

Acknowledgement

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

Contact information

Please contact your local Mitsubishi Electric representative.

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

1 https://cwe.mitre.org/data/definitions/319.html
2 https://www.first.org/cvss/v3.1/specification-document