

Denial-of-Service and Malicious Code Execution Vulnerability in MELSEC Series CPU module

Release date: May 23, 2023
Mitsubishi Electric Corporation

■ Overview

A Denial-of-Service and a Malicious Code Execution vulnerability exists in the MELSEC Series CPU modules. A remote attacker may cause a denial of service (DoS) condition or execute malicious code on a target product by sending specially crafted packets. However, the attacker needs to understand the internal structure of products to execute malicious code. Therefore, it is difficult to execute malicious code. (CVE-2023-1424)

■ CVSS¹

CVE-2023-1424 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H Base Score 10.0

■ Affected products

The following products are affected:

Series	Product name	Version
MELSEC iQ-F Series	FX5U-xMy/z x=32,64,80, y=T,R, z=ES,DS,ESS,DSS	Serial number 17X**** or later
	FX5UC-xMy/z x=32,64,96, y=T, z=D,DSS	Serial number 17X**** or later
	FX5UC-32MT/DS-TS, FX5UC-32MT/DSS-TS, FX5UC-32MR/DS-TS	

Please refer to the following manual for how to check the version.

- "15.3 Troubleshooting Using the Engineering Tool" - "Module diagnostics" in the MELSEC iQ-F FX5S/FX5UJ/FX5U/FX5UC User's Manual (Hardware)

Please download the manual from the following URL.

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

■ Description

A Denial-of-Service and a Malicious Code Execution vulnerability due to Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') (CWE-120²) exists in the MELSEC Series CPU modules.

■ Impact

A remote attacker may cause a denial of service (DoS) condition or execute malicious code on a target product by sending specially crafted packets. However, the attacker needs to understand the internal structure of products to execute malicious code. Therefore, it is difficult to execute malicious code. A system reset of the product is required for recovery from a denial of service (DoS) condition and malicious code execution.

■ Countermeasures

The following products have been fixed.

Series	Product name	Version
MELSEC iQ-F Series	FX5U-xMy/z x=32,64,80, y=T,R, z=ES,DS,ESS,DSS	Serial number 17X**** or later
	FX5UC-xMy/z x=32,64,96, y=T, z=D,DSS	Serial number 17X**** or later
	FX5UC-32MT/DS-TS, FX5UC-32MT/DSS-TS, FX5UC-32MR/DS-TS	

Please download a fixed firmware update file from the following site and update the firmware.

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

Please refer to the following product manual for how to update firmware.

- "5 FIRMWARE UPDATE FUNCTION" in the MELSEC iQ-F FX5 User's Manual (Application)

■ 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.

¹ <https://www.first.org/cvss/v3.1/specification-document>

² <https://cwe.mitre.org/data/definitions/120.html>

- Use IP filter function* to block access from untrusted hosts.
- Restrict physical access to the LAN that is connected by affected products.

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

■ Acknowledgement

Mitsubishi Electric would like to thank Matt Wiseman of Cisco Talos who reported this vulnerability.

■ Contact information

Please contact your local Mitsubishi Electric representative.

<Inquiries | MITSUBISHI ELECTRIC FA>

<https://www.mitsubishielectric.com/fa/support/index.html>