Multiple Denial-of-Service Vulnerabilities in MELSEC iQ-F Series CPU module

Release date: May 17, 2022
Last update date: May 31, 2022
Mitsubishi Electric Corporation

■Overview

Multiple Denial-of-Service (DoS) vulnerabilities exist in MELSEC iQ-F series CPU module. These vulnerabilities could allow a malicious attacker to cause a DoS condition for a product's program execution or communication. (CVE-2022-25161, CVE-2022-25162)

■CVSS

CVE-2022-25161 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H Base Score 8.6
CVE-2022-25162 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L Base Score 5.3

■Affected products

The following products and versions 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	Prior to 1.270
		Serial number 179**** and prior	Prior to 1.073
	FX5UC-xMy/z x=32,64,96, y=T,R, z=D,DSS	Serial number 17X**** or later	Prior to 1.270
		Serial number 179**** and prior	Prior to 1.073
	FX5UC-32MT/DS-TS, FX5UC-32MT/DSS-TS, FX5UC-32MR/DS-TS		Prior to 1.270
	FX5UJ-xMy/z x=24,40,60, y=T,R, z=ES,ESS		Prior to 1.030
	FX5UJ-xMy/ES-A* x=24,40,60, y=T,R		Prior to 1.031
	FX5S-xMy/z* x=30,40,60,80, y=T,R, z=ES,ESS		1.000

* These products are sold in limited regions

Please refer to the following user's manual for how to check the version.
"9.3 Troubleshooting using the engineering tool" in the MELSEC iQ-F FX5S/FX5UJ/FX5U/FX5UC User's Manual (Hardware)

■Description

Multiple DoS vulnerabilities below exist in MELSEC iQ-F series CPU module.
CVE-2022-25161: Improper Input Validation(CWE-20)
CVE-2022-25162: Improper Input Validation(CWE-20)

■Impact

These vulnerabilities could allow a malicious attacker to cause a DoS condition for a product's program execution or communication by sending specially crafted packets. For CVE-2022-25161, a system reset of the product is required for recovery.

■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	1.270 or later
		Serial number 179**** and prior	1.073 or later
	FX5UC-xMy/z x=32,64,96, y=T,R, z=D,DSS	Serial number 17X**** or later	1.270 or later
		Serial number 179**** and prior	1.073 or later
	FX5UC-32MT/DS-TS, FX5UC-32MT/DSS-TS, FX5UC-32MR/DS-TS		1.270 or later
	FX5UJ-xMy/z x=24,40,60, y=T,R, z=ES,ESS		1.030 or later
	FX5UJ-xMy/ES-A* x=24,40,60, y=T,R		1.031 or later
	FX5S-xMy/z* x=30,40,60,80, y=T,R, z=ES,ESS		1.001 or later

* These products are sold in limited regions. For how to get the fixed version of these products, please contact your local Mitsubishi Electric representative.

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

https://www.mitsubishielectric.com/fa/#software

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

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

- Use a firewall or virtual private network (VPN), etc. to prevent unauthorized access when Internet access is required.
- Use firewalls or IP filter function to restrict connections to the products and prevent access from untrusted networks or hosts. For details on IP filter function, refer to the following product manual.
  "12.1 IP Filter Function" in the MELSEC iQ-F FX5 User's Manual (Ethernet Communication)

■Acknowledgement

Mitsubishi Electric would like to thank Anton Dorfman of Positive Technologies who reported these vulnerabilities.

■Contact information

Please contact your local Mitsubishi Electric representative.

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

■Update history

May 31, 2022

Added the information of modules that have been fixed to "Affected products" and "Countermeasures".