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

Release date: May 23, 2023
Last update date: April 25, 2024
Mitsubishi Electric Corporation

Overview

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

CVSS[1]

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		Firmware 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	from 1.220 to 1.281
	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		
MELSEC iQ-R Series	R00/01/02CPU		35 and prior
	R04/08/16/32/120(EN)CPU		from 12 to 68
	R08/16/32/120SFCPU		from 26 to 31
	R08/16/32/120PCPU		from 3 to 37

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

- "17.3 Troubleshooting Using the Engineering Tool" – "Module diagnostics" in the MELSEC iQ-F FX5S/FX5UJ/FX5U/FX5UC User's Manual (Hardware)
- "Appendix 1 Checking Production Information and Firmware Version" in the MELSEC iQ-R Module Configuration Manual

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

Description

A Denial-of-Service and Remote Code Execution vulnerability due to Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') (CWE-120[2]) exists in the MELSEC Series CPU modules.

Impact

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

1 https://www.first.org/cvss/v3.1/specification-document
2 https://cwe.mitre.org/data/definitions/120.html

Countermeasures for Customers

<Customers using the affected CPU modules of MELSEC iQ-F Series>
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.
- "9 FIRMWARE UPDATE FUNCTION" in the MELSEC iQ-F FX5 User's Manual (Application)

<Customers using the affected CPU modules of MELSEC iQ-R series Safety(R08/16/32/120SFCPU) >
Take mitigations and workarounds.
We have released the fixed version as shown below, but updating the product to the fixed version is not available.

<Customers using the affected CPU modules of MELSEC iQ-R series except Safety(R08/16/32/120SFCPU) >
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.
- MELSEC iQ-R Module Configuration Manual “Appendix 2 Firmware Update Function”

Countermeasures for Products

The following products have been fixed.

Series	Product name		Firmware 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	1.290 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		
MELSEC iQ-R Series	R00/01/02CPU		36 or later
	R04/08/16/32/120(EN)CPU		69 or later
	R08/16/32/120SFCPU		32 or later
	R08/16/32/120PCPU		38 or later

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* 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.
"13.1 IP Filter Function" in the MELSEC iQ-F FX5 User's Manual (Communication)
"1.13 Security" - "IP filter" in the MELSEC iQ-R Ethernet User’s Manual(Application)

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

Update history

April 25, 2024
・Revised description regarding “Countermeasures”.

March 14, 2024
・Added modules that have been fixed to “Countermeasures”.
R08/16/32/120SFCPU

September 12, 2023
・Added modules that have been fixed to “Countermeasures”.

R08/16/32/120PCPU

July 6, 2023

・Added modules to “Affected products”.
R00/01/02CPU, R04/08/16/32/120(EN)CPU, R08/16/32/120SFCPU, R08/16/32/120PCPU

・Added modules that have been fixed to “Countermeasures”.
R00/01/02CPU, R04/08/16/32/120(EN)CPU