Denial-of-Service（DoS）Vulnerability in Web server function on MELSEC Series CPU module

Release date: November 2, 2023
Last Update date: February 15, 2024
Mitsubishi Electric Corporation

Overview

A denial-of-service (DoS) vulnerability exists in the Web server function of the MELSEC iQ-F/iQ-R Series CPU module. A remote attacker could prevent legitimate users from logging into the Web server function for a certain period after the attacker has attempted to log in illegally, by continuously attempting unauthorized login to the Web server function. The impact of this vulnerability will persist while the attacker continues to attempt unauthorized login. (CVE-2023-4625)

CVSS[1]

CVE-2023-4625 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 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**** and later	All versions
		Serial number 179**** and prior	1.060 or later
	FX5UC-xMy/z x=32,64,96, y=T, z=D,DSS	Serial number 17X**** and later	All versions
		Serial number 179**** and prior	1.060 or later
	FX5UC-32MT/DS-TS, FX5UC-32MT/DSS-TS, FX5UC-32MR/DS-TS		All versions
	FX5UJ-xMy/z x=24,40,60, y=T,R, z=ES,DS,ESS,DSS		All versions
	FX5UJ-xMy/ES-A* x=24,40,60, y=T,R		All versions
	FX5S-xMy/z x=30,40,60,80, y=T,R, z=ES,ESS		All versions
MELSEC iQ-R Series	R00/01/02CPU		05 or later
	R04/08/16/32/120(EN)CPU		35 or later
	R08/16/32/120PCPU		37 or later

* These products are sold in limited regions.

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)
- "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(DoS) vulnerability due to Improper Restriction of Excessive Authentication Attempts（CWE-307[2]） exists in the Web server function of the MELSEC iQ-F/iQ-R Series CPU module.

Impact

A remote attacker could prevent legitimate users from logging into the Web server function for a certain period after the attacker has attempted to log in illegally by continuously attempting unauthorized login to the Web server function. The impact of this vulnerability will persist while the attacker continues to attempt unauthorized login.

Countermeasures

Please carry out 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.

1 https://www.first.org/cvss/v3.1/specification-document
2 https://cwe.mitre.org/data/definitions/307.html

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

*: For details on the 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)
"1.13 Security" – "IP Filter" in the MELSEC iQ-R Ethernet User's Manual (Application)

Acknowledgement

Mitsubishi Electric would like to thank Peter Cheng from ELEX FEIGONG RESEARCH INSTITUTE of Elex Cybersecurity, Inc. 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

February 15, 2024
- The following series have been added to the affected products.
  MELSEC iQ-R Series
- The "Overview", "Affected products", "Description", and "Mitigation/Workarounds" have been revised.