

Authentication Bypass Vulnerability in WEB Server Function on MELSEC Series

Release date: January 17, 2023
 Last update date: January 26, 2023
 Mitsubishi Electric Corporation

■ Overview

An authentication bypass vulnerability exists in the WEB server function of the MELSEC iQ-F/iQ-R Series. An unauthenticated remote attacker may be able to access the WEB server function by guessing the random numbers used for authentication from several used random numbers (CVE-2022-40267).

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

■ CVSS¹

CVE-2022-40267 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N Base Score 5.9

■ 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	1.280 and prior
		Serial number 179**** and prior	1.074 and prior
	FX5UC-xMy/z x=32,64,96, y=T, z=D,DSS	Serial number 17X**** or later	1.280 and prior
		Serial number 179**** and prior	1.074 and prior
	FX5UC-32MT/DS-TS, FX5UC-32MT/DSS-TS, FX5UC-32MR/DS-TS		1.280 and prior
	FX5UJ-xMy/z x=24,40,60, y=T,R, z=ES,ESS		1.042 and prior
	FX5UJ-xMy/ES-A* x=24,40,60, y=T,R		1.043 and prior
FX5S-xMy/z* x=30,40,60,80, y=T,R, z=ES,ESS		1.003 and prior	
MELSEC iQ-R Series	R00/01/02CPU	All versions	
	R04/08/16/32/120(EN)CPU	All versions	

* 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

An authentication bypass vulnerability exists in the WEB server function of the MELSEC iQ-F/iQ-R Series due to predictable seed in pseudo-random number generator(CWE-337²).

■ Impact

An unauthenticated remote attacker may be able to access the WEB server function by guessing the random numbers used for authentication from several used random numbers.

■ Countermeasures

The following products have been fixed. Mitsubishi Electric will fix other products in the near future.

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	1.281 or later
		Serial number 179**** and prior	1.075 or later
	FX5UC-xMy/z x=32,64,96, y=T, z=D,DSS	Serial number 17X**** or later	1.281 or later
		Serial number 179**** and prior	1.075 or later
	FX5UC-32MT/DS-TS, FX5UC-32MT/DSS-TS, FX5UC-32MR/DS-TS		1.281 or later
	FX5UJ-xMy/z x=24,40,60, y=T,R, z=ES,ESS		1.044 or later
	FX5UJ-xMy/ES-A* x=24,40,60, y=T,R		1.045 or later
FX5S-xMy/z* x=30,40,60,80, y=T,R, z=ES,ESS		1.004 or later	

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

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

² <https://cwe.mitre.org/data/definitions/337.html>

Please download 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.
- Use IP filter function* to block access from untrusted hosts.

*: 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 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

January 26, 2023

Added modules(FX5UJ, FX5UJ-A, FX5S CPU module) to “Affected products”.

Added modules(FX5UJ, FX5UJ-A, FX5S CPU module) that have been fixed to “Countermeasures”.

Modified “authorization” to “authentication” in title, “Overview” and “Description”.