

Information Disclosure Vulnerability in MELSEC Series

Release date: March 2, 2023
Mitsubishi Electric Corporation

■ Overview

An information disclosure vulnerability due to Plaintext Storage of Password(CWE-256¹) exists in MELSEC iQ-F Series. An unauthenticated attacker may be able to login to FTP server or Web server by obtaining plaintext credentials stored in project files. (CVE-2023-0457)

■ CVSS²

CVE-2023-0457 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N Base score:7.5

■ Affected products

The following products are affected:

Series	Product name	Version
MELSEC iQ-F Series	FX5U(C) CPU modules, All models	All version
	FX5UJ CPU modules, All models	All version
	FX5S CPU modules, All models	All version
	FX5-ENET	All version
	FX5-ENET/IP	All version

■ Description

An information disclosure vulnerability due to Plaintext Storage of a Password(CWE-256) exists in MELSEC iQ-F Series.

■ Impact

An unauthenticated attacker may be able to login to FTP server or Web server by obtaining plaintext credentials stored in project files.

■ 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:

- Encrypt the communication data or project files when sending and receiving or sharing these files.
- 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 affected products.

*: 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)

■ Acknowledgement

Mitsubishi Electric would like to thank JeongHoon Bae, YiJoon Jung, JinYoung Kim, HyeokJong Yun and HeeA Go of HelloT 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>

¹ <https://cwe.mitre.org/data/definitions/256.html>

² <https://www.first.org/cvss/v3.1/specification-document>