Multiple Vulnerabilities in MELSEC iQ-R Series/iQ-F Series EtherNet/IP Modules and EtherNet/IP Configuration tool

Release date: June 1, 2023
Mitsubishi Electric Corporation

■Overview

Multiple vulnerabilities exist in MELSEC iQ-R Series/iQ-F Series EtherNet/IP modules and EtherNet/IP configuration tools.

Due to improper handling of the password for the FTP function on EtherNet/IP modules, a remote unauthenticated attacker may connect to the module via FTP and bypass authentication to log in illegally.(CVE-2023-2060, CVE-2023-2061, CVE-2023-2062)

Alternatively, since the FTP function on EtherNet/IP module does not restrict file upload/download, an attacker may be able to disclose, tamper with, delete, or destroy information. As a result, a remote attacker may be able to exploit this for further attacks.(CVE-2023-2063)

The model names and firmware versions affected by these vulnerabilities are listed below. Please carry out the following mitigations/workarounds.

■CVSS[1]

CVE-2023-2060	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	Base Score:7.5
CVE-2023-2061	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	Base Score:6.2
CVE-2023-2062	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	Base Score:6.2
CVE-2023-2063	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L	Base Score:6.3

■Affected products

The following products are affected:

Product Name	Version	Explanation
RJ71EIP91	All versions	MELSEC iQ-R Series EtherNet/IP module
SW1DNN-EIPCT-BD	All versions	RJ71EIP91 EtherNet/IP configuration tool
FX5-ENET/IP	All versions	MELSEC iQ-F Series EtherNet/IP module
SW1DNN-EIPCTFX5-BD	All versions	FX5-ENET/IP EtherNet/IP configuration tool

■Description

Following vulnerabilities exist in the affected products.

- Authentication bypass vulnerability in FTP function on EtherNet/IP module due to Weak Password Requirements(CWE-521)[2] allows a remote unauthenticated attacker to access to the module via FTP by dictionary attack or password sniffing. (CVE-2023-2060)
- Authentication bypass vulnerability in FTP function on EtherNet/IP module due to Use of Hard-coded Password(CWE-259)[3] allows a remote unauthenticated attacker to obtain a hard-coded password and access to the module via FTP. (CVE-2023-2061)
- The EtherNet/IP configuration tool that displays unmasked password due to Missing Password Field Masking(CWE-549)[4] results in authentication bypass vulnerability, which allows a remote unauthenticated attacker to access the module via FTP. (CVE-2023-2062)
- Information disclosure, tampering, deletion, destruction vulnerability exists in the FTP function on EtherNet/IP module via file upload/download due to Unrestricted Upload of File with Dangerous Type(CWE-434)[5]. (CVE-2023-2063)

■Impact

A remote unauthenticated attacker may connect to the module via FTP and bypass authentication to log in illegally. Alternatively, after login, an attacker can freely upload/download files, disclose communication settings, and tamper with/delete/destroy communication settings. Depending on the nature of the tampering, communication may stop after the module is restarted, unintended communication may occur, and further attacks may occur.

■Countermeasures

Please carry out mitigations/workarounds.

■Mitigations/Workarounds

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

- Use a firewall, 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.
- Restrict physical access to prevent untrusted devices LAN to which the affected product connects.
- Avoid uploading/downloading files directly using FTP, and use the EtherNet/IP configuration tool. Also, do not open the downloaded file with anything other than the EtherNet/IP configuration tool.
- For FX5-ENET/IP, use IP filter function to block access from untrusted hosts. For details on the IP filter function, please refer to

[1] https://www.first.org/cvss/v3.1/specification-document

[2] https://cwe.mitre.org/data/definitions/521.html

[3] https://cwe.mitre.org/data/definitions/259.html

[4] https://cwe.mitre.org/data/definitions/549.html

[5] https://cwe.mitre.org/data/definitions/434.html

the following manual.
"12.1 IP Filter Function" in the MELSEC iQ-F FX5 User's Manual (Ethernet Communication)

■Acknowledgement

Mitsubishi Electric would like to thank Iie Karada 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