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

Release date: June 1, 2023
Last update date: April 25, 2024
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.

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	Applicable CVE ID	Explanation
RJ71EIP91	All versions	**CVE-2023-2060** **CVE-2023-2061** **CVE-2023-2063**	MELSEC iQ-R Series EtherNet/IP module
FX5-ENET/IP	All versions	**CVE-2023-2060** **CVE-2023-2061** **CVE-2023-2063**	MELSEC iQ-F Series EtherNet/IP module
SW1DNN-EIPCT-BD	**Software version "1.01B" and prior**	**CVE-2023-2062**	RJ71EIP91 EtherNet/IP configuration tool
SW1DNN-EIPCTFX5-BD	All versions	**CVE-2023-2062**	FX5-ENET/IP EtherNet/IP configuration tool

<How to check the version>
RJ71EIP91 : Refer to "Appendix 1 Checking Production Information and Firmware Version " in the "MELSEC iQ-R Module Configuration Manual".
SW1DNN-EIPCT-BD : Refer to "3.4 Checking the Software Version" in the "MELSEC iQ-R EtherNet/IP Module User's Manual (Application)".

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

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

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 for Customers

Customers who are using the affected products are requested to take the following actions.

Product Name	Countermeasures for Customers
RJ71EIP91	There are no plans to release a fixed version, so please take mitigations and workarounds below. In addition, please consider replacing to the next generation model, CC-Link IE TSN Plus Master/Local Module RJ71GN11-EIP.
FX5-ENET/IP	Please take mitigations and workarounds below.
SW1DNN-EIPCT-BD	Please download and update the fixed version listed in the next section from the following site. https://www.mitsubishielectric.com/fa/#software
SW1DNN-EIPCTFX5-BD	Please take mitigations and workarounds below.

Countermeasures for Products

The product name and versions that have been fixed are as follows.

Product Name	Versions
SW1DNN-EIPCT-BD	Software version "1.02C" or later

Mitigations / Workarounds

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

<Common to RJ71EIP91 and FX5-ENET/IP>

- 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.

<RJ71EIP91 firmware version "06" or later>

- FTP function can be disabled in firmware version "06" or later. Except when configuring with the EtherNet/IP Configuration Tool, to prevent unauthorized access from outside, set the connection to "Deny connection" in the EtherNet/IP Configuration Tool Connection Permission Change function and disable the EtherNet/IP module's FTP function of the EtherNet/IP module. For detailed configuration instructions, please refer to the following manuals. However, firmware versions earlier than "06" cannot be updated to version "06" or later.

MELSEC iQ-R EtherNet/IP Module User's Manual (Application) "1.3 Ethernet/IP Configuration Tool Connectable Function".

<FX5-ENET/IP>

- For FX5-ENET/IP, use IP filter function to block access from untrusted hosts. For details on the IP filter function, please refer to the following manual.

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

<Common to SW1DNN-EIPCT-BD and SW1DNN-EIPCTFX5-BD>

- Take the above mitigation and workaround measures in RJ71EIP91 and FX5-ENET/IP.
- Allow only trusted users to log in or remotely log in.
- Make sure that no one else sneaks a peek at the screen of a user from behind while using the product.
- If you leave your desk while using the product, lock your PC and prevent others from using it.
- Use the PC using the product within a LAN and block access from untrusted networks or hosts.
- Restrict physical access to the PC on which the product is installed as well as the PCs and network devices that can communicate with the product.
- Install antivirus software on the PCs that use the product and on the PCs that can communicate with the product.
- Do not open untrusted files or click on untrusted links.

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

Update history

April 25, 2024

- **"Countermeasures" were divided into "Countermeasures for Customers" and "Countermeasures for Products"**
- **Added modules that have been fixed to "Countermeasures for Products".**
  SW1DNN-EIPCT-BD
- **"Mitigations/Workarounds" were divided into descriptions for each affected product, and added following product version information in the "Mitigations and Workarounds".**
  RJ71EIP91 firmware version "06" or later