ICSA-23-157-02

Mitsubishi Electric MELSEC iQ-R Series/iQ-F Series

1. EXECUTIVE SUMMARY

CVSS v3 7.5

- **ATTENTION**: Exploitable remotely/low attack complexity
- **Vendor**: Mitsubishi Electric
- **Equipment**: MELSEC iQ-R Series/iQ-F Series EtherNet/IP Modules and EtherNet/IP Configuration tool
- **Vulnerabilities:** Weak Password Requirements, Use of Hard-coded Credentials, Missing Password Field Masking, Unrestricted Upload of File with Dangerous Type

2. RISK EVALUATION

Successful exploitation of these vulnerabilities could allow a remote unauthenticated attacker to connect to the module via FTP and bypass authentication to log in.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

Mitsubishi Electric reports these vulnerabilities affect the following MELSEC iQ-R Series/iQ-F Series EtherNet/IP Modules and EtherNet/IP Configuration tool:

- RJ71EIP91: All versions (CVE-2023-2060, CVE-2023-2061, CVE-2023-2063)
- FX5-ENET/IP: All versions (CVE-2023-2060, CVE-2023-2061, CVE-2023-2063)
- SW1DNN-EIPCT-BD: version "1.01B" and prior (CVE-2023-2062)
- SW1DNN-EIPCTFX5-BD: All versions (CVE-2023-2062)

3.2 Vulnerability Overview

3.2.1 Weak Password Requirements CWE-521

Authentication bypass vulnerability in FTP function on EtherNet/IP module due to weak password requirements allows a remote unauthenticated attacker to access to the module via FTP by dictionary attack or password sniffing.

CVE-2023-2060 has been assigned to this vulnerability. A CVSS v3 base score of 7.5 has been calculated; the CVSS vector string is (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).

A CVSS v4 score has been calculated for CVE-2023-2060. A base score of 8.7 has been calculated; the CVSS vector string is (CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N).

3.2.2 Use of Hard-coded Credentials CWE-798

Authentication bypass vulnerability in FTP function on EtherNet/IP module due to use of hard-coded credentials allows a remote unauthenticated attacker to obtain a hard-coded password and access to the module via FTP.

CVE-2023-2061 has been assigned to this vulnerability. A CVSS v3 base score of 6.2 has been calculated; the CVSS vector string is (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).

A CVSS v4 score has been calculated for CVE-2023-2061. A base score of 6.9 has been calculated; the CVSS vector string is (CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N).

3.2.3 Missing Password Field Masking CWE-549

The EtherNet/IP configuration tool that displays unmasked password due to missing password field masking results in authentication bypass vulnerability, which allows a remote unauthenticated attacker to access the module via FTP.

CVE-2023-2062 has been assigned to this vulnerability. A CVSS v3 base score of 6.2 has been calculated; the CVSS vector string is (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).

A CVSS v4 score has been calculated for CVE-2023-2062. A base score of 6.9 has been calculated; the CVSS vector string is (CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N).

3.2.4 Unrestricted Upload of File with Dangerous Type CWE-434

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.

CVE-2023-2063 has been assigned to this vulnerability. A CVSS v3 base score of 6.3 has been

calculated; the CVSS vector string is (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L).

A CVSS v4 score has been calculated for CVE-2023-2063. A base score of 5.3 has been calculated; the CVSS vector string is (CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N).

3.3 BACKGROUND

- **CRITICAL INFRASTRUCTURE SECTORS:** Critical Manufacturing
- **COUNTRIES/AREAS DEPLOYED:** Worldwide
- **COMPANY HEADQUARTERS LOCATION:** Japan

3.4 RESEARCHER

Iie Karada reported these vulnerabilities to Mitsubishi Electric.

4. MITIGATIONS

Mitsubishi Electric recommends that users of the affected products take the following actions.:

- RJ71EIP91: Consider replacing to the next generation model, CC-Link IE TSN Plus Master/Local Module RJ71GN11-EIP.
- 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).
- SW1DNN-EIPCT-BD: Download and update the fixed version Software version "1.02C" or later
- 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. However, firmware versions earlier than "06" cannot be updated to version "06" or later. For detailed configuration instructions, please refer to the following manuals: MELSEC iQ-R EtherNet/IP Module User's Manual (Application) "1.3 Ethernet/IP Configuration Tool Connectable Function".

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.

Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting these vulnerabilities common to SW1DNN-EIPCT-BD and SW1DNN-EIPCTFX5-BD:

- Take the above mitigation 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

For specific update instructions and additional details see the Mitsubishi Electric advisory.

CISA recommends users take defensive measures to minimize the risk of exploitation of these vulnerabilities. CISA reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

CISA also provides a section for control systems security recommended practices on the ICS webpage on cisa.gov. Several CISA products detailing cyber defense best practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

CISA encourages organizations to implement recommended cybersecurity strategies for proactive defense of ICS assets. Additional mitigation guidance and recommended practices are publicly

available on the ICS webpage at cisa.gov in the technical information paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies.

Organizations observing suspected malicious activity should follow established internal procedures and report findings to CISA for tracking and correlation against other incidents.

No known public exploits specifically target these vulnerabilities. These vulnerabilities are exploitable remotely. These vulnerabilities have low attack complexity.

5. PUBLICATION HISTORY

- June 6, 2023: Initial Publication
- April 25, 2024: Updated with new mitigation information.