Malicious Code Execution Vulnerability in Multiple FA Engineering Software Products

Release date: July 30, 2020
Last update date: April 11, 2023
Mitsubishi Electric Corporation

■ Overview

Multiple Mitsubishi Electric FA engineering software products have a malicious code execution vulnerability. A malicious attacker could use this vulnerability to obtain information, tamper the information, cause a denial-of-service (DoS), and so on. The product names and versions affected by the vulnerability are listed below.

■ Affected Products

<Products and Versions>
C Controller Interface Module utility, versions 2.00 and prior
CC-Link IE Control Network Data Collector, version 1.00A
CC-Link IE Field Network Data Collector, version 1.00A
CC-Link IE TSN Data Collector, version 1.00A
CPU Module Logging Configuration Tool, versions 1.100E and prior
CW Configurator, versions 1.010L and prior
Data Transfer, versions 3.42U and prior
EZSocket, versions 5.1 and prior
FR Configurator SW3, all versions
FR Configurator2, versions 1.26C and prior
GT Designer2 Classic, all versions
GT Designer3 Version1 (GOT1000), versions 1.241B and prior
GT Designer3 Version1 (GOT2000), versions 1.241B and prior
GT SoftGOT1000 Version3, versions 3.200J and prior
GT SoftGOT2000 Version1, versions 1.241B and prior
GX Developer, versions 8.504A and prior
GX LogViewer, versions 1.100E and prior
GX Works2, versions 1.601B and prior
GX Works3, versions 1.063R and prior
M_CommDTM-IO-Link, versions 1.03D and prior
MELFA-Works, versions 4.4 and prior
MELSEC WinCPU Setting Utility, all versions
MELSOFT Complete Clean Up Tool, versions 1.06G and prior
MELSOFT EM Software Development Kit, versions 1.015R and prior
MELSOFT iQ AppPortal, versions 1.17T and prior
MELSOFT Navigator, versions 2.74C and prior
MI Configurator, versions 1.004E and prior
Motion Control Setting, versions 1.005F and prior
Motorizer, versions 1.005F and prior
MR Configurator2, versions 1.125F and prior
MT Works2, versions 1.167Z and prior
MTConnect Data Collector, versions 1.1.4.0 and prior
MX Component, versions 4.20W and prior
MX MESInterface, versions 1.21X and prior
MX MESInterface-R, versions 1.12N and prior
MX Sheet, version 2.15R and prior
Network Interface Board CC IE Control utility, versions 1.29F and prior
Network Interface Board CC IE Field Utility, versions 1.16S and prior
Network Interface Board CC-Link Ver.2 Utility, versions 1.23Z and prior
Network Interface Board MNETH utility, versions 34L and prior
Position Board utility 2, versions 3.20 and prior
PX Developer, versions 1.53F and prior
RT ToolBox2, versions 3.73B and prior
RT ToolBox3, versions 1.82L and prior
Setting/monitoring tools for the C Controller module (SW3PVC-CCPU), versions 3.13P and prior
Setting/monitoring tools for the C Controller module (SW4PVC-CCPU), versions 4.12N and prior

SLMP Data Collector, version 1.04E and prior

<How to Check the Versions>
Refer to the manual or help of each product.

■ Description
Multiple Mitsubishi Electric FA engineering software products have a malicious code execution vulnerability (CVE-2020-14521). This is because some files in the product have improper permissions, and a malicious attacker could replace them with malicious files (CWE-428).

■ Impact
A malicious attacker could use this vulnerability to obtain information, tamper the information, cause a denial-of-service (DoS), and so on.

■ Countermeasures
Download the latest version of each software product from the following site and update it:
https://www.mitsubishielectric.com/fa/#software

The fixed software products and versions are as follows:

<Products and Versions>
C Controller Interface Module utility, version 2.10 or later
CC-Link IE Control Network Data Collector, version 1.01B or later
CC-Link IE Field Network Data Collector, version 1.01B or later
CC-Link IE TSN Data Collector, version 1.01B or later
CPU Module Logging Configuration Tool, version 1.106K or later
CW Configurator, version 1.011M or later
Data Transfer, version 3.43V or later
EZSocket, version 5.2 or later (*1)
FR Configurator2, version 1.27D or later
GT Designer3 Version1 (GOT1000), version 1.245F or later
GT Designer3 Version1 (GOT2000), version 1.245F or later
GT SoftGOT1000 Version3, version 3.245F or later
GT SoftGOT2000 Version1, version 1.245F or later
GX Developer, version 8.505B or later
GX LogViewer, version 1.106K or later
GX Works2, version 1.605F or later
GX Works3, version 1.065T or later
M_CommDTM-IO-Link, version 1.04E or later
MELFA-Works, version 4.5 or later
MELSOFT Complete Clean Up Tool, version 1.07H or later
MELSOFT EM Software Development Kit, version 1.020W or later
MELSOFT iQ AppPortal, version 1.20W or later
MELSOFT Navigator, version 2.78G or later
MI Configurator, version 1.005F or later
Motion Control Setting, version 1.006G or later
Motorizer, version 1.010L or later
MR Configurator2, version 1.130L or later
MT Works2, version 1.170C or later
MTConnect Data Collector, version 1.1.5.0 or later (*2)
MX Component, version 4.21X or later
MX MESInterface, version 1.22Y or later
MX MESInterface-R, version 1.13P or later
MX Sheet, version 2.16S or later
Network Interface Board CC IE Control Utility, version 1.30G or later
Network Interface Board CC IE Field Utility, version 1.17T or later
Network Interface Board CC-Link Ver.2 Utility, version 1.24A or later
Network Interface Board MNETH Utility, version 35M or later
Position Board utility 2, version 3.30 or later
PX Developer, version 1.54G or later
RT ToolBox2, version 3.74C or later

RT ToolBox3, version 1.90U or later
Setting/monitoring tools for the C Controller module (SW3PVC-CCPU), version 3.14Q or later
Setting/monitoring tools for the C Controller module (SW4PVC-CCPU), version 4.13P or later
SLMP Data Collector, version 1.05F or later

Mitsubishi Electric recommends the following actions for FR Configurator SW3 (setting tool for 700 series Inverter module), GT Designer2 Classic (screen creation software for GOT900 series HMI module) and MELSEC WinCPU Setting Utility (setting tool for MELSEC-Q series WinCPU module) because there are no countermeasure version release for these products.

- FR Configurator SW3 : Migrate to 800 series Inverter module that is the successor model and FR Configurator 2 (SW1DND-FRC2-E).
- GT Designer2 Classic : Migrate to GOT2000 series HMI module that is the successor model and GT Designer3 Version1(GOT2000) (SW1DND-GTWK3-EC).
- MELSEC WinCPU Setting Utility : Migrate to MELSEC iQ-R series MELSEC WinCPU module that is the successor model and setting tool CW Configurator (SW1DND-RCCPU-E).

<How to Update the Products>
Refer to the manual or help of each product.

(*1) EZSocket is a communication middleware product for Mitsubishi Electric partner companies. Mitsubishi Electric will directly provide the fixed version to the partner companies.
(*2) For MTConnect Data Collector, please contact your local Mitsubishi Electric representative.

■ Mitigations
For customers who are using a product that has not released a fixed version or who cannot immediately update the product, Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:

-If a "File Name Warning" message is displayed when starting Windows, take appropriate measures according to the instructions in the message, such as changing a file name, and then install or operate the products.
-Operate the products under an account that does not have administrator's privileges.
-Install an antivirus software in your personal computer using the products.
-Restrict network exposure for all control system devices or systems to the minimum necessary, and ensure that they are not accessible from untrusted networks and hosts.
-Locate control system networks and remote devices behind firewalls and isolate them from the business network.
-Use Virtual Private Network (VPN) when remote access is required.

■ Acknowledgements
Mitsubishi Electric would like to thank Mashav Sapir of Claroty who reported this vulnerability.

■ Contact Information
Please contact your local Mitsubishi Electric representative.

■ Update history
April 11, 2023
Added recommended actions for FR Configurator SW3, GT Designer2 Classic and MELSEC WinCPU Setting Utility to "Countermeasures".

March 2, 2023
Added Position Board utility 2 that has been fixed to "Countermeasures".

November 17, 2022
Added C Controller Interface Module utility and MELSOFT EM Software Development Kit that have been fixed to "Countermeasures".

July 28, 2022
Added MI Configurator, Setting/monitoring tools for the C Controller module (SW3PVC-CCPU) and Setting/monitoring tools for the C Controller module (SW4PVC-CCPU) that have been fixed to "Countermeasures".

May 24, 2022
Added FR Configurator2, M_CommDTM-IO-Link, Network Interface Board CC IE Control Utility, Network Interface Board CC IE

Field Utility, Network Interface Board CC-Link Ver.2 Utility and Network Interface Board MNETH Utility that have been fixed to "Countermeasures".

February 8, 2022

Added CC-Link IE Control Network Data Collector, CC-Link IE Field Network Data Collector, CC-Link IE TSN Data Collector, MR Configurator2, MT Works2, MTConnect Data Collector and SLMP Data Collector that have been fixed to "Countermeasures".

November 16, 2021

Added MELFA-Works, RT ToolBox2 and RT ToolBox3 that have been fixed to "Countermeasures".
Added CC-Link IE TSN Data Collector to "Affected Products"

July 27, 2021

Added GX Works2, MELSOFT Complete Clean Up Tool and MELSOFT Navigator that have been fixed to "Countermeasures".

May 27, 2021

Added EZSocket and PX Developer that have been fixed to "Countermeasures".

January 14, 2021

Added MELSOFT iQ AppPortal, MX Component and MX Sheet that have been fixed to "Countermeasures".

November 5, 2020

Added Data Transfer, GT Designer3 Version1(GOT1000), GT Designer3 Version1(GOT2000), GT SoftGOT1000 Version3, GT SoftGOT2000 Version1, MX MESInterface, and MX MESInterface-R that have been fixed to "Countermeasures".