Malicious Code Execution Vulnerability in Multiple FA Engineering Software Products

Release date: July 30, 2020
Last update date: January 14, 2021
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, all versions
C Controller module setting and monitoring tool, all versions
CC-Link IE Control Network Data Collector, all versions
CC-Link IE Field Network Data Collector, all versions
CPU Module Logging Configuration Tool, version 1.100E and prior
CW Configurator, version 1.010L and prior
Data Transfer, version 3.42U and prior
EZSocket, all versions
FR Configurator SW3, all versions
FR Configurator2, all versions
GT Designer2 Classic, all versions
GT Designer3 Version1 (GOT1000), version 1.241B and prior
GT Designer3 Version1 (GOT2000), version 1.241B and prior
GT SoftGOT1000 Version3, version 3.200J and prior
GT SoftGOT2000 Version1, version 1.241B and prior
GX Developer, version 8.504A and prior
GX LogViewer, version 1.100E and prior
GX Works2, all versions
GX Works3, version 1.063R and prior
M_CommDTM-IO-Link, all versions
MELFA-Works, all versions
MELSEC WinCPU Setting Utility, all versions
MELSOFT Complete Clean Up Tool, all versions
MELSOFT EM Software Development Kit, all versions
MELSOFT iQ AppPortal, version 1.17T and prior
MELSOFT Navigator, all versions
MI Configurator, all versions
Motion Control Setting, version 1.005F and prior
Motorizer, version 1.005F and prior
MR Configurator2, all versions
MT Works2, all versions
MTConnect Data Collector, all versions
MX Component, version 4.20W and prior
MX MESInterface, version 1.21X and prior
MX MESInterface-R, version 1.12N and prior
MX Sheet, version 2.15R and prior
Network Interface Board CC IE Control utility, all versions
Network Interface Board CC IE Field Utility, all versions
Network Interface Board CC-Link Ver.2 Utility, all versions
Network Interface Board MNETH utility, all versions
Position Board utility 2, all versions
PX Developer, all versions
RT ToolBox2, all versions
RT ToolBox3, all versions
Setting/monitoring tools for the C Controller module, all versions
SLMP Data Collector, all versions

<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>
CPU Module Logging Configuration Tool, version 1.106K or later
CW Configurator, version 1.011M or later
Data Transfer, version 3.43V 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 Works3, version 1.065T or later
MELSOFT iQ AppPortal, version 1.20W or later
Motion Control Setting, version 1.006G or later
Motorizer, version 1.010L or later
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

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

■ 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

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”.