Vulnerability due to Improper File Access Control in Multiple FA Engineering Software Products

Release date: July 30, 2020
Last update date: September 22, 2022
Mitsubishi Electric Corporation

■Overview

Multiple Mitsubishi Electric FA engineering software products have a vulnerability due to improper file access control. A malicious attacker who successfully exploited this vulnerability could escalate privilege and execute malicious programs, which could allow information to be disclosed, tampered with or destroyed, or denial-of-service (DoS).
The product names and versions affected by the vulnerability are listed below.

■Affected Products

<Products and Versions>
CPU Module Logging Configuration Tool, versions 1.100E and prior
CW Configurator, versions 1.010L and prior
Data Transfer, versions 3.40S and prior
EZSocket, versions 4.5 and prior
FR Configurator2, versions 1.22Y and prior
GT Designer3 Version1 (GOT2000), versions 1.235V and prior
GT SoftGOT1000 Version3, 3.200J and prior
GT SoftGOT2000 Version1, versions 1.235V and prior
GX LogViewer, versions 1.100E and prior
GX Works2, versions 1.592S and prior
GX Works3, versions 1.063R and prior
M_CommDTM-HART, version 1.00A
M_CommDTM-IO-Link, versions 1.03D and prior
MELFA-Works, versions 4.3 and prior
MELSEC WinCPU Setting Utility, versions 1.03D and prior
MELSOFT EM Software Development Kit (EM Configurator), versions 1.010L and prior
MELSOFT FieldDeviceConfigurator, versions 1.03D and prior
MELSOFT Navigator, versions 2.62Q and prior
MH11 SettingTool Version2, versions 2.002C and prior
MI Configurator, versions 1.004E and prior
Motorizer, versions 1.005F and prior
MR Configurator2, versions 1.105K and prior
MT Works2, versions 1.156N and prior
MX Component, versions 4.19V 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
PX Developer, versions 1.52E and prior
RT ToolBox2, versions 3.72A and prior
RT ToolBox3, versions 1.70Y and prior
Setting/monitoring tools for the C Controller module (SW4PVC-CCPU), versions 4.12N 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 vulnerability that a malicious attacker could replace with crafted files due to improper permissions (CWE-275) on some files in the products (CVE-2020-14496). Executing the replaced files by a user with administrator privileges may result in information disclosure, information tampering/destruction, or denial-of-service (DoS).

■Impact

A malicious attacker who successfully exploited this vulnerability could escalate privilege and execute malicious programs, which could allow information to be disclosed, tampered with or destroyed, or denial-of-service (DoS).

■Countermeasures

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 3.41T or later
EZSocket, version 4.6 or later (*1)
FR Configurator2, version 1.23Z or later (*2)
GT Designer3 Version1 (GOT2000), version 1.236W or later
GT SoftGOT1000 Version3, version 3.245F or later
GT SoftGOT2000 Version1, version 1.236W or later
GX LogViewer, version 1.106K or later
GX Works2, version 1.595V or later
GX Works3, version 1.065T or later
M_CommDTM-HART, version 1.01B or later
M_CommDTM-IO-Link, version 1.04E or later
MELFA-Works, version 4.4 or later
MELSEC WinCPU Setting Utility (*3)
MELSOFT EM Software Development Kit (EM Configurator), version 1.015R or later
MELSOFT FieldDeviceConfigurator, version 1.04E or later
MELSOFT Navigator, version 2.70Y or later
MH11 SettingTool Version2, version 2.003D or later
MI Configurator, version 1.005F or later
Motorizer, version 1.010L or later
MR Configurator2, version 1.106L or later
MT Works2, version 1.160S or later
MX Component, version 4.20W 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
PX Developer, version 1.53F or later
RT ToolBox2, version 3.73B or later
RT ToolBox3, version 1.80J or later
Setting/monitoring tools for the C Controller module (SW4PVC-CCPU), version 4.13P or later

<How to Get the Fixed Versions>
Download the latest version of each software product from the following site and update it(Excluding *1 and *2 products):
https://www.mitsubishielectric.com/fa/#software

(*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) Download FR Configurator2 fixed version from the following URL:
https://www.mitsubishielectric.com/fa/download/software/drv/inv/vulnerability-protection/index.html

(*3) Mitsubishi Electric recommends that customers migrate to the MELSEC iQ-R series MELSEC WinCPU module that is the successor model and setting tool CW Configurator (SW1DND-RCCPU-E) because there is no countermeasure version release for MELSEC WinCPU Setting Utility (setting tool for MELSEC-Q series WinCPU module).

<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:

-Install the fixed version GX Works2, GX Works3, or MELSOFT Navigator on the PC on which the product is installed. This is because these three products provide comprehensive countermeasures that give the same countermeasure effect to other products installed in the same folder (e.g. C:¥Program files¥MELSOFT).

-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 Younes Dragoni of Nozomi Networks, Applied Risk research team and Mashav Sapir of Claroty who reported this vulnerability.

■Contact Information

Please contact your local Mitsubishi Electric representative.

■Update history

September 22 2022

Added countermeasure for MELSEC WinCPU Setting Utility to "Countermeasures".

July 28, 2022

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

Setting/monitoring tools for the C Controller module (SW3PVC-CCPU) has been removed from "Affected Products".

May 24, 2022

Added 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".

December 17, 2020

Added GT SoftGOT1000 Version3 that have been fixed to "Countermeasures".