Malicious Code Execution Vulnerability in Multiple FA Products

Release date: July 30, 2020
Last update date: July 28, 2022
Mitsubishi Electric Corporation

■ Overview

Multiple Mitsubishi Electric FA products have a vulnerability that a malicious attacker could execute arbitrary code due to path traversal.

The product names and versions affected by the vulnerability are listed below.

■ Affected Products

<Products and Versions>
CW Configurator, versions 1.010L and prior
FR Configurator2, versions 1.22Y and prior
GX Works2, versions 1.595V and prior
GX Works3, versions 1.063R and prior
MELSEC iQ-R Series Motion Module, versions 10 and prior
MELSOFT iQ AppPortal, versions 1.17T and prior
MELSOFT Navigator, versions 2.70Y and prior
MI Configurator, versions 1.004E and prior
MR Configurator2, versions 1.110Q and prior
MT Works2, versions 1.156N and prior
MX Component, versions 4.20W and prior
RT ToolBox3, versions 1.70Y and prior

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

■ Description

Multiple Mitsubishi Electric FA products have a vulnerability (CVE-2020-14523) that a malicious attacker could execute arbitrary code due to path traversal (CWE-22).

■ Impact

By operating a project file/configuration data file that has been crafted by a malicious attacker, customers may be affected as follows:

- If the customer has administrator privileges, it is possible to rewrite arbitrary executable files and library files by the action of the project file or the configuration data file. As a result, the attacker can rewrite executable files and library files to arbitrary code and execute them.

■ Countermeasures

The fixed software products and versions are as follows:

<Products and Versions>
CW Configurator, version 1.011M or later
FR Configurator2, version 1.23Z or later (*1)
GX Works2, version 1.596W or later
GX Works3, version 1.065T or later
MELSEC iQ-R Series Motion Module, version 12 or later
MELSOFT iQ AppPortal, version 1.20W or later
MELSOFT Navigator, version 2.74C or later
MI Configurator, version 1.005F or later
MR Configurator2, version 1.115V or later
MT Works2, version 1.160S or later
MX Component, version 4.21X or later
RT ToolBox3, version 1.80J 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):
https://www.mitsubishielectric.com/fa/#software

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

<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:

-Make sure that the file is obtained from the correct acquisition route when customers receive a project file or a configuration data file from another person via mail, USB memory, file server, etc. (Or, check that there is no file of unknown source.)
-Operate the products under an account that does not have administrator's privileges. (Except for MELSEC iQ-R Series Motion Module.)
-Install an antivirus software in your personal computer using the products. (Except for MELSEC iQ-R Series Motion Module.)
-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

July 28, 2022
Added MI Configurator that has been fixed to “Countermeasures”.

May 27, 2021
Added MELSEC iQ-R Series Motion Module that has been fixed to “Countermeasures”.

January 14, 2021
Added MELSOFT iQ AppPortal, MELSOFT Navigator, MR Configurator2 and MX Component that have been fixed to “Countermeasures”.