Multiple Vulnerabilities Due to Improper Handling of XML in Multiple FA Engineering Software Products

June 30, 2020
Mitsubishi Electric Corporation

■Overview

There are multiple vulnerabilities due to improper handling of XML in multiple Mitsubishi Electric FA engineering software products. These vulnerabilities could allow a malicious attacker to send a file on the computer running the product to the outside or cause the product to enter a denial-of-service condition.
The product names and versions affected by these vulnerabilities are listed below. Please update to the fixed versions.

■Affected Products

<Products and Versions>
CPU Module Logging Configuration Tool, versions 1.94Y and prior
CW Configurator, versions 1.010L and prior
EM Software Development Kit (EM Configurator), versions 1.010L and prior
GT Designer3(GOT2000), versions 1.221F and prior
GX LogViewer, versions 1.96A and prior
GX Works2, versions 1.586L and prior
GX Works3, versions 1.058L and prior
M_CommDTM-HART, version 1.00A
M_CommDTM-IO-Link, versions 1.02C and prior
MELFA-Works, versions 4.3 and prior
MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool, versions 1.004E and prior
MELSOFT FieldDeviceConfigurator, versions 1.03D and prior
MELSOFT iQ AppPortal, versions 1.11M and prior
MELSOFT Navigator, versions 2.58L and prior
MI Configurator, versions 1.003D and prior
Motion Control Setting, versions 1.005F and prior
MR Configurator2, versions 1.72A and prior
MT Works2, versions 1.156N and prior
RT ToolBox2, versions 3.72A and prior
RT ToolBox3, versions 1.50C 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 the following multiple vulnerabilities due to improper handling of XML:

-Improper Restriction of XML External Entity Reference (CWE-611) - CVE-2020-5602
The vulnerability could allow a malicious attacker to send a file on the computer running the product to the outside.

-Uncontrolled Resource Consumption (CWE-400) - CVE-2020-5603
The vulnerability could allow a malicious attacker to cause the product to enter a denial-of-service condition.

■Impact

When customers use a project file or a configuration data file that has been specially crafted by a malicious attacker, they can be affected as follows:
-Any file that can be accessed with user privileges is sent externally.
-The product enters a denial-of-service condition.

■Countermeasures

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

The fixed versions are as follows:

<Products and Versions>
CPU Module Logging Configuration Tool, version 1.100E or later
CW Configurator, version 1.011M or later
EM Software Development Kit (EM Configurator), version 1.015R or later
GT Designer3(GOT2000), version 1.225K or later
GX LogViewer, version 1.100E or later
GX Works2, version 1.590Q or later
GX Works3, version 1.060N or later
M_CommDTM-HART, version 1.01B or later
M_CommDTM-IO-Link, version 1.03D or later
MELFA-Works, version 4.4 or later
MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool,version 1.005F or later
MELSOFT FieldDeviceConfigurator, version 1.04E or later
MELSOFT iQ AppPortal, version 1.14Q or later
MELSOFT Navigator, version 2.62Q or later
MI Configurator, version 1.004E or later
Motion Control Setting, version 1.006G or later
MR Configurator2, version 1.100E or later
MT Works2, version 1.160S or later
RT ToolBox2, version 3.73B or later
RT ToolBox3, version 1.60N or later

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

■Mitigations

For customers who cannot immediately update the software products, Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting these vulnerabilities:

-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 administrators 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.

■Contact Information

Please contact your local Mitsubishi Electric representative.