Multiple Denial-of-Service Vulnerabilities in Multiple FA Engineering Software Products

Release date: February 18, 2021
Mitsubishi Electric Corporation

■Overview

Multiple Mitsubishi Electric FA engineering software products have multiple Denial-of-Service vulnerabilities. If a malicious attacker sends specially crafted packets and the software products receive the packets, the attacker may cause a Denial-of-Service (DoS) of the software products. (CVE-2021-20587, CVE-2021-20588)

■CVSS

CVE-2021-20587: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Base Score:7.5
CVE-2021-20588: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H Base Score:7.5

■Affected products

<Products and Versions>
-C Controller module setting and monitoring tool (*1), all versions
-CPU Module Logging Configuration Tool (*1), all versions
-CW Configurator (*1), all versions
-Data Transfer (*1), all versions
-EZSocket (*1)(*2)(*3), all versions
-FR Configurator (*2), all versions
-FR Configurator SW3 (*2), all versions
-FR Configurator2 (*2), all versions
-GT Designer3 Version1(GOT1000)(*3), all versions
-GT Designer3 Version1(GOT2000)(*3), all versions
-GT SoftGOT1000 Version3 (*3), all versions
-GT SoftGOT2000 Version1 (*3), all versions
-GX Configurator-DP (*1), versions 7.14Q and prior
-GX Configurator-QP (*1), all versions
-GX Developer (*1), all versions
-GX Explorer (*1), all versions
-GX IEC Developer (*1), all versions
-GX LogViewer (*1), all versions
-GX RemoteService-I (*1), all versions
-GX Works2 (*1), versions 1.597X and prior
-GX Works3 (*1), versions 1.070Y and prior
-M_CommDTM-HART (*1), all versions
-M_CommDTM-IO-Link (*1), all versions
-MELFA-Works (*1), all versions
-MELSEC WinCPU Setting Utility (*1), all versions
-MELSOFT EM Software Development Kit (EM Configurator) (*1), all versions
-MELSOFT Navigator (*1) (*2) (*3), all versions
-MH11 SettingTool Version2 (*1), all versions
-MI Configurator (*1), all versions
-MT Works2 (*1), all versions
-MX Component (*1) (*2) (*3), all versions
-Network Interface Board CC IE Control utility (*1), all versions
-Network Interface Board CC IE Field Utility (*1), all versions
-Network Interface Board CC-Link Ver.2 Utility (*1), all versions
-Network Interface Board MNETH utility (*1), all versions
-PX Developer (*1), all versions
-RT ToolBox2 (*1), all versions
-RT ToolBox3 (*1), all versions
-Setting/monitoring tools for the C Controller module (*1), all versions
-SLMP Data Collector (*1), all versions

(*1) The software product that communicate with MELSEC products. MELSEC is the brand name of PLC products manufactured by Mitsubishi Electric.
(*2) The software product that communicate with FREQROL products. FREQROL is the brand name of Inverter products manufactured by Mitsubishi Electric.
(*3) The software product that communicate with GOT products. GOT is the brand name of HMI products manufactured by

Mitsubishi Electric.

■Description

Multiple Mitsubishi Electric FA engineering software products have multiple vulnerabilities below. If these vulnerabilities are exploited by malicious attackers, the software products may enter Denial-of-Service (DoS) condition.

Heap-based Buffer Overflow (CWE-122) CVE-2021-20587

Improper Handling of Length Parameter Inconsistency (CWE-130) CVE-2021-20588

■Impact

A malicious attacker may cause a Denial-of-Service (DoS) of the software products by spoofing MELSEC, GOT or FREQROL and returning crafted reply packets. In addition, the attacker may execute a malicious program on the personal computer running the software products, although have not been reproduced.

■Countermeasures

The fixed software products and versions are as follows:

<Products and Versions>

-GX Configurator-DP, version 7.15R or later

-GX Works2, version 1.600A or later

-GX Works3, version 1.072A or later

<How to Get the Fixed Versions>

Download the latest version of each software product from the following site and update it:

https://www.mitsubishielectric.com/fa/#software

<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 mitigations to minimize the risk of exploiting this vulnerability:

-Install the fixed version of GX Works3 on your personal computer running the products when communicating with MELSEC (*4). Because GX Works3 provide comprehensive countermeasures that give the same countermeasure effect to other products.

-Operate the products under an account that does not have administrator's privileges.

-Install an antivirus software in your personal computer running 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.

(*4) Fixed software products that communicate with GOT and FREQROL are currently under development.

■Acknowledgement

Mitsubishi Electric would like to thank dliangfun who reported these vulnerabilities.

■Contact information

Please contact your local Mitsubishi Electric representative.

< Inquiries | MITSUBISHI ELECTRIC FA >

https://www.mitsubishielectric.com/fa/support/index.html