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

Release date:February 18, 2021
Last update date:November 17, 2022
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>

-CPU Module Logging Configuration Tool (*1), versions 1.112R and prior
-CW Configurator (*1), versions 1.011M and prior
-Data Transfer (*3), versions 3.44W and prior
-EZSocket (*1)(*2)(*3), versions 5.4 and prior
-FR Configurator (*2), all versions
-FR Configurator SW3 (*2), all versions
-FR Configurator2 (*2), versions 1.24A and prior
-GT Designer3 Version1(GOT1000)(*3), versions 1.250L and prior
-GT Designer3 Version1(GOT2000)(*3), versions 1.250L and prior
-GT SoftGOT1000 Version3 (*3), versions 3.245F and prior
-GT SoftGOT2000 Version1 (*3), versions 1.250L and prior
-GX Configurator-DP (*1), versions 7.14Q and prior
-GX Configurator-QP (*1), all versions
-GX Developer (*1), versions 8.506C and prior
-GX Explorer (*1), all versions
-GX IEC Developer (*1), all versions
-GX LogViewer (*1), versions 1.115U and prior
-GX RemoteService-I (*1), all versions
-GX Works2 (*1), versions 1.597X and prior
-GX Works3 (*1), versions 1.070Y and prior
-iQ Monozukuri ANDON (Data Transfer (*3)), all versions
-iQ Monozukuri Process Remote Monitoring (Data Transfer (*3)), all versions
-M_CommDTM-HART (*1), all versions
-M_CommDTM-IO-Link (*1), versions 1.03D and prior
-MELFA-Works (*1), versions 4.4 and prior
-MELSEC WinCPU Setting Utility (*1), all versions
-MELSOFT EM Software Development Kit (EM Configurator) (*1), versions 1.015R and prior
-MELSOFT Navigator (*1) (*2) (*3), versions 2.74C and prior
-MH11 SettingTool Version2 (*1), versions 2.004E and prior
-MI Configurator (*1), versions 1.004E and prior
-MT Works2 (*1), versions 1.167Z and prior
-MX Component (*1) (*2) (*3), versions 5.001B and prior
-Network Interface Board CC IE Control utility (*1), versions 1.29F and prior
-Network Interface Board CC IE Field Utility (*1), versions 1.16S and prior
-Network Interface Board CC-Link Ver.2 Utility (*1), versions 1.23Z and prior
-Network Interface Board MNETH utility (*1), versions 34L and prior
-PX Developer (*1), versions 1.53F and prior
-RT ToolBox2 (*1), versions 3.73B and prior
-RT ToolBox3 (*1), versions 1.82L and prior
-Setting/monitoring tools for the C Controller module (SW4PVC-CCPU) (*1), versions 4.12N and prior
-SLMP Data Collector (*1), versions 1.04E and prior

(*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>
-CPU Module Logging Configuration Tool, version 1.118X or later
-CW Configurator, version 1.012N or later
-Data Transfer, version 3.45X or later(*4)
-EZSocket, version 5.5 or later(*5)
-FR Configurator2, version 1.25B or later
-GT Designer3 Version1(GOT1000), version 1.255R or later
-GT Designer3 Version1(GOT2000), version 1.255R or later
-GT SoftGOT1000 Version3, version 3.255R or later
-GT SoftGOT2000 Version1, version 1.255R or later
-GX Configurator-DP, version 7.15R or later(*6)
-GX Developer, version 8.507D or later
-GX LogViewer, version 1.118X or later
-GX Works2, version 1.600A or later
-GX Works3, version 1.072A or later
-M_CommDTM-IO-Link, version 1.04E or later
-MELFA-Works, version 4.5 or later
-MELSOFT EM Software Development Kit (EM Configurator), version 1.020W or later
-MELSOFT Navigator, version 2.78G or later
-MH11 SettingTool Version2, version 2.005F or later
-MI Configurator, version 1.005F or later
-MT Works2, version 1.170C or later
-MX Component, version 5.002C 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 1.54G or later
-RT ToolBox2, version 3.74C or later
-RT ToolBox3, version 1.90U or later
-Setting/monitoring tools for the C Controller module (SW4PVC-CCPU), version 4.13P or later
-SLMP Data Collector, version 1.05F 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.

(*4) For updating the iQ Monozukuri ANDON and iQ Monozukuri Process Remote Monitoring, download the fixed version of Data Transfer in advance.
(*5) Mitsubishi Electric will directly provide the fixed version of EZSocket to the partner companies.
(*6) Please contact your local Mitsubishi Electric representative about GX Configurator-DP.

■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. Because GX Works3 provide comprehensive countermeasures that give the same countermeasure effect to other products.
-Install the fixed version of FR Configurator2 on your personal computer running the products when communicating with FREQROL. Because FR Configurator2 provide comprehensive countermeasures that give the same countermeasure effect to other products.
-Install the fixed version of GT Designer3 on your personal computer running the products when communicating with GOT. Because GT Designer3 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.

■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

■Update history

November 17, 2022
Added fixed product as below
MELSOFT EM Software Development Kit (EM Configurator)

July 28, 2022
Added fixed products as below
EZSocket, MI Configurator, Setting/monitoring tools for the C Controller module (SW4PVC-CCPU)
Setting/monitoring tools for the C Controller module (SW3PVC-CCPU) has been removed from "Affected Products"

May 24, 2022
Added fixed products as below
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, Network Interface Board MNETH Utility

February 8, 2022
Added fixed products as below
MT Works2, MX Component, SLMP Data Collector

November 16, 2021
Added fixed products as below
MELFA-Works, MH11 SettingTool Version2, RT ToolBox2

July 27, 2021
Added fixed products as below
GX Developer, MELSOFT Navigator

May 27, 2021
Added fixed products as below
CPU Module Logging Configuration Tool, CW Configurator, Data Transfer, FR Configurator2, GT Designer3 Version1(GOT1000), GT Designer3 Version1(GOT2000), GT SoftGOT1000 Version3, GT SoftGOT2000 Version1, GX LogViewer, PX Developer, RT ToolBox3
Added Affected products as below
iQ Monozukuri ANDON (Data Transfer), iQ Monozukuri Process Remote Monitoring (Data Transfer)