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

Release date:February 18, 2021
Last update date:June 5, 2025
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) condition on the software products. (CVE-2021-20587, CVE-2021-20588)

CVSS[1]

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

The affected products and versions are as follows.

Product name	Version
CPU Module Logging Configuration Tool (*1)	"1.112R" and prior
CW Configurator (*1)	"1.011M" and prior
Data Transfer (*3)	"3.44W" and prior
EZSocket (*1)(*2)(*3)	"5.4" and prior
FR Configurator (*2)	All versions
FR Configurator SW3 (*2)	All versions
FR Configurator2 (*2)	"1.24A" and prior
GT Designer3 Version1(GOT1000) (*3)	"1.250L" and prior
GT Designer3 Version1(GOT2000) (*3)	"1.250L" and prior
GT SoftGOT1000 Version3 (*3)	"3.245F" and prior
GT SoftGOT2000 Version1 (*3)	"1.250L" and prior
GX Configurator-DP (*1)	"7.14Q" and prior
GX Configurator-QP (*1)	All versions
GX Developer (*1)	"8.506C" and prior
GX Explorer (*1)	All versions
GX IEC Developer (*1)	All versions
GX LogViewer (*1)	"1.115U" and prior
GX RemoteService-I (*1)	All versions
GX Works2 (*1)	"1.597X" and prior
GX Works3 (*1)	"1.070Y" and prior
iQ Monozukuri ANDON (Data Transfer (*3))	"1.003D" and prior
iQ Monozukuri Process Remote Monitoring (Data Transfer (*3))	"1.002C" and prior
M_CommDTM-HART (*1)	All versions
M_CommDTM-IO-Link (*1)	"1.03D" and prior
MELFA-Works (*1)	"4.4" and prior
MELSEC WinCPU Setting Utility (*1)	All versions
MELSOFT EM Software Development Kit (EM Configurator) (*1)	"1.015R" and prior
MELSOFT Navigator (*1)(*2)(*3)	"2.74C" and prior
MH11 SettingTool Version2 (*1)	"2.004E" and prior
MI Configurator (*1)	"1.004E" and prior
MT Works2 (*1)	"1.167Z" and prior
MX Component (*1)(*2)(*3)	"5.001B" and prior
Network Interface Board CC IE Control utility (*1)	"1.29F" and prior
Network Interface Board CC IE Field Utility (*1)	"1.16S" and prior
Network Interface Board CC-Link Ver.2 Utility (*1)	"1.23Z" and prior
Network Interface Board MNETH utility (*1)	"34L" and prior
PX Developer (*1)	"1.53F" and prior
RT ToolBox2 (*1)	"3.73B" and prior
RT ToolBox3 (*1)	"1.82L" and prior
Setting/monitoring tools for the C Controller module (SW4PVC-CCPU) (*1)	"4.12N" and prior
SLMP Data Collector (*1)	"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.

[1] https://www.first.org/cvss/v3.1/specification-document

(*3) The software product that communicate with GOT products. GOT is the brand name of HMI products manufactured by Mitsubishi Electric.

<How to Check the Versions>
Please refer to the manual or help documentation for each product.

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[2]) CVE-2021-20587
Improper Handling of Length Parameter Inconsistency (CWE-130[3]) CVE-2021-20588

Impact

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

Countermeasures for Customers

- Customers using the affected products for which countermeasure versions are listed in "Countermeasures for Products"
Please download and install the update from the following site.
https://www.mitsubishielectric.com/fa/download/index.html

- Customers using the affected products for which countermeasure versions are not listed in "Countermeasures for Products"
There are no plans to release fixed versions for the following product:
FR Configurator
FR Configurator SW3
GX Configurator-QP
GX Explorer
GX IEC Developer
GX RemoteService-I
M_CommDTM-HART
MELSEC WinCPU Setting Utility
Please take the following “Mitigations/Workarounds”.

Countermeasures for Products

The following products have been fixed Multiple Denial-of-Service Vulnerabilities.

Product name	Version
CPU Module Logging Configuration Tool	"1.118X" or later
CW Configurator	"1.012N" or later
Data Transfer	"3.45X" or later
EZSocket (*4)	"5.5" or later
FR Configurator2	"1.25B" or later
GT Designer3 Version1(GOT1000)	"1.255R" or later
GT Designer3 Version1(GOT2000)	"1.255R" or later
GT SoftGOT1000 Version3	"3.255R" or later
GT SoftGOT2000 Version1	"1.255R" or later
GX Configurator-DP (*5)	"7.15R" or later
GX Developer	"8.507D" or later
GX LogViewer	"1.118X" or later
GX Works2	"1.600A" or later
GX Works3	"1.072A" or later
iQ Monozukuri ANDON (Data Transfer)	"1.004E" or later
iQ Monozukuri Process Remote Monitoring (Data Transfer)	"1.005F" or later
M_CommDTM-IO-Link	"1.04E" or later
MELFA-Works	"4.5" or later
MELSOFT EM Software Development Kit (EM Configurator)	"1.020W" or later
MELSOFT Navigator	"2.78G" or later
MH11 SettingTool Version2	"2.005F" or later
MI Configurator	"1.005F" or later
MT Works2	"1.170C" or later
MX Component	"5.002C" or later
Network Interface Board CC IE Control utility	"1.30G" or later
Network Interface Board CC IE Field Utility	"1.17T" or later
Network Interface Board CC-Link Ver.2 Utility	"1.24A" or later

2 https://cwe.mitre.org/data/definitions/122.html
3 https://cwe.mitre.org/data/definitions/130.html

Product name	Version
Network Interface Board MNETH utility	"35M" or later
PX Developer	"1.54G" or later
RT ToolBox2	"3.74C" or later
RT ToolBox3	"1.90U" or later
Setting/monitoring tools for the C Controller module (SW4PVC-CCPU)	"4.13P" or later
SLMP Data Collector	"1.05F" or later

(*4) Mitsubishi Electric will directly provide the fixed version of EZSocket to the partner companies.
(*5) Please contact your local Mitsubishi Electric representative about GX Configurator-DP.

Mitigations / Workarounds

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

June 5, 2025
Divided "Countermeasures" into "Countermeasures for Customers" and "Countermeasures for Products".
Added products for which there are no plans for release fixed versions to the "Countermeasures for Customers" section.
Added the updated products to the "Countermeasures for Products" section.
iQ Monozukuri ANDON (Data Transfer)
iQ Monozukuri Process Remote Monitoring (Data Transfer)

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)