Malicious Code Execution Vulnerability in FA Engineering Software Products

Release date: September 19, 2023
Last update date: July 4, 2024
Mitsubishi Electric Corporation

Overview

Malicious Code Execution Vulnerability due to Incorrect Default Permissions (CWE-276[1]) exists in Multiple FA engineering software products when installed in a folder other than the default installation folder. This vulnerability could allow a malicious local attacker to execute a malicious code, which could result in information disclosure, tampering with and deletion, or a denial-of-service (DoS) condition.

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

CVSS[2]

CVE-2023-4088 CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H Base Score:9.3

Affected products

The following products and versions are affected:

< Products and Versions >
- AL-PCS/WIN-E, all versions
- CPU Module Logging Configuration Tool, all versions
- EZSocket, all versions
- FR Configurator2, all versions
- FX Configurator-EN, all versions
- FX Configurator-EN-L,all versions
- FX Configurator-FP, all versions
- GT Designer3 Version1(GOT1000), all versions
- GT Designer3 Version1(GOT2000), all versions
- GT SoftGOT1000 Version3, all versions
- GT SoftGOT2000 Version1, all versions
- GX LogViewer, all versions
- GX Works2, all versions
- GX Works3, all versions
- MELSOFT FieldDeviceConfigurator, all versions
- MELSOFT iQ AppPortal, all versions
- MELSOFT MaiLab, all versions
- MELSOFT Navigator, all versions
- MELSOFT Update Manager, all versions
- MX Component, all versions
- MX Sheet, all versions
- PX Developer, all versions
- RT ToolBox3, all versions
- RT VisualBox, all versions
- Data Transfer, all versions
- Data Transfer Classic, all versions

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

Description

Malicious Code Execution Vulnerability due to Incorrect Default Permissions (CWE-276) exists in Multiple FA engineering software products when installed in a folder other than the default installation folder. However, if the products is installed in the default installation folder, this vulnerability does not affect the products.

Impact

This vulnerability could allow a malicious local attacker to execute a malicious code, which could result in information disclosure, tampering with and deletion, or a denial-of-service (DoS) condition.

[1] https://cwe.mitre.org/data/definitions/276.html

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

Countermeasures

There are no plans to release fixed versions. Please carry out mitigations/workarounds.

Mitigations / Workarounds

Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:

- Install into the default installation folder. However, for the following products, the following versions or later (*) must be used.

(*) Products with following versions and prior are vulnerable to CVE-2020-14496[3], and the mitigation measures are not effective.

Products Name	Versions
CPU Module Logging Configuration Tool	Ver. 1.106K
EZSocket	Ver. 4.6
FR Configurator2	Ver. 1.23Z
GT Designer3 Version1(GOT2000)	Ver. 1.236W
GT SoftGOT1000 Version3	Ver. 3.245F
GT SoftGOT2000 Version1	Ver. 1.236W
GX LogViewer	Ver. 1.106K
GX Works2	Ver. 1.595V
GX Works3	Ver. 1.065T
MELSOFT FieldDeviceConfigurator	Ver. 1.04E
MELSOFT Navigator	Ver. 2.70Y
MX Component	Ver. 4.20W
RT ToolBox3	Ver. 1.80J
Data Transfer	Ver. 3.41T

- If it is necessary to change the installation folder from the default, select a folder that only users with Administrator privileges have permission to change.
- Install an antivirus software in your personal computer using the affected product.
- Use your personal computer with the affected product within the LAN and block remote login from untrusted networks, hosts, and users.
- When connecting your perconal computer with the affected product to the Internet, use a firewall, virtual private network (VPN), etc., to prevent unauthorized access, and allow only trusted users to remote login.
- Don't open untrusted files or click untrusted links.

Acknowledgement

Mitsubishi Electric would like to thank 01dGu0 of ZHEJIANG QIAN INFORMATION & TECHNOLOGY CO., LTD. who reported this vulnerability.

Contact information

Please contact your local Mitsubishi Electric representative.
<Inquiries | MITSUBISHI ELECTRIC FA>
https://www.mitsubishielectric.com/fa/support/index.html

Update history

July 4, 2024

Added Affected products.

AL-PCS/WIN-E, CPU Module Logging Configuration Tool, EZSocket, FR Configurator2, FX Configurator-EN, FX Configurator-EN-L, FX Configurator-FP, GT Designer3 Version1(GOT1000), GT Designer3 Version1(GOT2000), GT SoftGOT1000 Version3, GT SoftGOT2000 Version1, GX LogViewer, GX Works2, MELSOFT FieldDeviceConfigurator, MELSOFT iQ AppPortal, MELSOFT MaiLab, MELSOFT Navigator, MELSOFT Update Manager, MX Component, MX Sheet, PX Developer, RT ToolBox3, RT VisualBox, Data Transfer, Data Transfer Classic

"Overview", "Description", and "Mitigations / Workarounds" are updated along with the addition of Affected products.

[3] https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-006_en.pdf