Authentication Bypass Vulnerability and Remote Code Execution Vulnerability in Multiple FA Engineering Software Products

Release date: January 30, 2024
Last update date: February 13, 2025
Mitsubishi Electric Corporation

Overview

Authentication bypass vulnerability due to Missing Authentication for Critical Function (CWE-306[1]) and remote code execution vulnerability due to Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') (CWE-470[2]) exist in multiple FA engineering software products. A remote unauthenticated attacker may be able to bypass authentication by sending specially crafted packets and connect to the products illegally. Furthermore, the attacker may be able to execute malicious code by remotely calling a function with a path to a malicious library while connected to the products. As a result, unauthorized users may disclose, tamper with, destroy or delete information in the products, or cause a denial-of-service (DoS) condition on the products. (CVE-2023-6942, CVE-2023-6943)

The product names and versions affected by these vulnerabilities are as follows.

CVSS[3]

CVE-2023-6942	CVSS v3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N	Base Score: 7.5
CVE-2023-6943	CVSS v3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	Base Score: 9.8

Affected products

The affected products and versions are as follows.

Product name	Versions
EZSocket	3.0 to 5.92
GT Designer3 Version1(GOT1000)	1.325P and prior
GT Designer3 Version1(GOT2000)	1.320J and prior
GX Works2	1.11M and later
GX Works3	1.106L and prior
MELSOFT Navigator	1.04E to 2.102G
MT Works2	1.190Y and prior
MX Component	4.00A to 5.007H
MX OPC Server DA/UA (Software packaged with MC Works64)	All versions

<How to Check the Versions>

Please refer to the manual or help documentation of each product.

Description

The following two vulnerabilities exist in multiple FA engineering software products:

CVE ID	Description of vulnerabilities
CVE-2023-6942	Authentication bypass vulnerability due to Missing Authentication for Critical Function (CWE-306)
CVE-2023-6943	Remote Code Execution Vulnerability due to Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') (CWE-470)

Impact

A remote unauthenticated attacker may be able to bypass authentication by sending specially crafted packets and connect to the products illegally (CVE-2023-6942). Furthermore, the attacker may be able to execute malicious code by remotely calling a function with a path to a malicious library while connected to the products (CVE-2023-6943). As a result, unauthorized users may disclose, tamper with, destroy or delete information in the products, or cause a denial-of-service (DoS) condition on the products.

[1] https://cwe.mitre.org/data/definitions/306.html

[2] https://cwe.mitre.org/data/definitions/470.html

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

Countermeasures for Customers

Please check the table in the next section, "Countermeasures for Products," to see if a fixed version has been released for your product.

<To customers using products for which the fixed version has been released>

Please download the fixed version mentioned in the next section from the following website and proceed with the update.

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

[Update Instructions]
Extract the downloaded file (in zip format).
Run setup.exe in the extracted folder to perform the installation.

<To customers using products for which the fixed version has not been released>

Please carry out mitigations/workarounds.

Please note that there are no plans to release fixed versions of the following product:

MX OPC Server DA/UA (Software packaged with MC Works64)

Countermeasures for Products

The fixed products and versions are as follows.

Product name	Fixed version
EZSocket	5.A or later
GT Designer3 Version1(GOT1000)	1.330U or later
GT Designer3 Version1(GOT2000)	1.325P or later
GX Works3	1.110Q or later
MELSOFT Navigator	2.106L or later
MT Works2	1.195D or later
MX Component	5.008J or later

Mitigations / Workarounds

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

- When connecting your personal computer with the affected products to the internet, use a firewall, virtual private network (VPN), etc., to prevent unauthorized access and allow only trusted users to remote login.
- Use your personal computer with the affected products within a LAN and block access from untrusted networks and hosts.
- Restrict physical access to your computer using the affected products as well as to the personal computers and network devices that can communicate with it.
- Install antivirus software on your personal computer using the affected products and on the personal computers that can communicate with it.
- Don’t open untrusted files or click untrusted links.

Acknowledgement

Mitsubishi Electric would like to thank Reid Wightman, Dragos Inc. 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

February 13, 2025
Added GT Designer3 Version1 (GOT1000) to "Countermeasures for Products"

January 16, 2025
Added EZSocket, GT Designer3 Version1 (GOT2000), MELSOFT Navigator, MT Works2 and MX Component to "Countermeasures for Products"

October 31, 2024
Removed FR Configurator2 from “Affected products”
Added “Countermeasures for Customers” section
Added “Countermeasures for Products” section and added fixed products