

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

Release date: January 30, 2024
Mitsubishi Electric Corporation

Overview

Authentication bypass vulnerability due to Missing Authentication for Critical Function (CWE-306¹) and remote code execution vulnerability due to Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') (CWE-470²) 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 a 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.

CVSS³

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 and later
FR Configurator2	All versions
GT Designer3 Version1(GOT1000)	All versions
GT Designer3 Version1(GOT2000)	All versions
GX Works2	1.11M and later
GX Works3	All versions
MELSOFT Navigator	1.04E and later
MT Works2	All versions
MX Component	4.00A and later
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 a 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.

Countermeasures

Please carry out mitigations/workarounds.

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>

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 this vulnerability.

Contact information

Please contact your local Mitsubishi Electric representative.

<Inquiries | MITSUBISHI ELECTRIC FA>

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