複数の FA エンジニアリングソフトウェア製品における
認証回避の脆弱性および悪意のあるプログラムが実行される脆弱性

公開日 2024 年 1 月 30 日
三菱電機株式会社

■概要

複数の FA エンジニアリングソフトウェア製品において、重要な機能に対する認証の欠如(CWE-306[1])に起因する認証回避の脆弱性およびクラスまたはコードを選択する外部から制御された入力の使用(CWE-470[2])に起因する悪意のあるプログラムが実行される脆弱性が存在することが判明しました。攻撃者は、細工したパケットを送信することにより、認証を回避して当該製品と不正に接続できる可能性があります。更に、当該製品との接続状態において、悪意のあるライブラリへのパスを指定して関数呼び出しを行うことにより、悪意のあるプログラムを実行できる可能性があります。結果として、権限のないユーザによって情報を窃取されたり、情報を改ざん・破壊・削除されたり、当該製品をサービス停止(DoS)状態に陥らさせられる可能性があります(CVE-2023-6942、CVE-2023-6943)。

この問題の影響を受けるソフトウェア製品およびバージョンを以下に示します。

■CVSS スコア [3]

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

■該当製品の確認方法

影響を受ける製品は、以下の通りです。

製品名	バージョン
EZSocket	Ver.3.0 以降
FR Configurator2	全バージョン
GT Designer3 Version1(GOT1000)	全バージョン
GT Designer3 Version1(GOT2000)	全バージョン
GX Works2	Ver.1.11M 以降
GX Works3	全バージョン
MELSOFT Navigator	Ver.1.04E 以降
MT Works2	全バージョン
MX Component	Ver4.00A 以降
MX OPC Server DA/UA (MC Works64 同梱ソフトウェア)	全バージョン

<バージョンの確認方法>
各製品のマニュアルまたはヘルプをご参照ください。

■脆弱性の説明

複数の FA エンジニアリングソフトウェア製品には、以下の 2 件の脆弱性が存在します。

CVE ID	脆弱性の説明
CVE-2023-6942	重要な機能に対する認証の欠如(CWE-306)に起因する認証回避の脆弱性
CVE-2023-6943	クラスまたはコードを選択する外部から制御された入力の使用(CWE-470)に起因する悪意のあるプログラムが実行される脆弱性

■脆弱性がもたらす脅威

攻撃者は、細工したパケットを送信することにより、認証を回避して当該製品と不正に接続できる可能性があります(CVE-2023-6942)。更に、当該製品との接続状態において、悪意のあるライブラリへのパスを指定して関数呼び出しを行うことにより、悪意のあるプログラムを実行できる可能性があります(CVE-2023-6943)。結果として、権限のないユーザによって情報を窃取されたり、情報を改ざん・破壊・削除されたり、当該製品をサービス停止(DoS)状態に陥らさせられる可能性があります。

■対策方法

軽減策・回避策にて対応をお願いいたします。

1 https://cwe.mitre.org/data/definitions/306.html
2 https://cwe.mitre.org/data/definitions/470.html
3 https://www.ipa.go.jp/security/vuln/CVSSv3.html

■軽減策・回避策

本脆弱性が悪用されることによるリスクを最小限に抑えるため、三菱電機は以下に示す軽減策を講じることを推奨します。

・当該製品を使用するパソコンをインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク（VPN）等で不正アクセスを防止したうえで、信頼できるユーザのみにリモートログインを許可する。

・当該製品を使用するパソコンを LAN 内で使用し、信頼できないネットワークやホストからのアクセスをブロックする。

・当該製品を使用するパソコンならびに当該製品と通信可能なパソコンおよびネットワーク機器への物理的なアクセスを制限する。

・当該製品を使用するパソコンおよび当該製品と通信可能なパソコンにウイルス対策ソフトを搭載する。

・信頼できないファイルを開いたり、信頼できないリンクをクリックしない。

■謝辞

これらの脆弱性をご報告いただいた Dragos 社 Reid Wightman 様に感謝いたします。

■お客様からのお問い合わせ先

製品をご購入いただいた当社の支社、代理店にご相談ください。

〈お問い合わせ | 三菱電機 FA〉

https://www.mitsubishielectric.co.jp/fa/support/purchase/index.html