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

公開日 2023 年 9 月 19 日
最終更新日 2024 年 7 月 4 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、デフォルト以外のインストールフォルダにインストールされている場合に、不適切なデフォルトパーミッション(CWE-276[1])により、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。
本脆弱性を悪意のある攻撃者に悪用された場合に、悪意のあるプログラムが実行され、情報を取得される、情報を改ざん・破壊・削除される、サービス停止(DoS)状態にされる等の可能性があります。
この問題の影響を受けるソフトウェア製品名およびバージョンを以下に示します。

■CVSS スコア [2]
CVE-2023-4088　CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H 基本値:9.3

■該当製品の確認方法
本脆弱性の影響を受ける製品は以下の製品です。
<製品とバージョン>
AL-PCS/WIN-E 全バージョン
CPU ユニットロギング設定ツール 全バージョン
EZSocket 全バージョン
FR Configurator2 全バージョン
FX Configurator-EN 全バージョン
FX Configurator-FP 全バージョン
FX3U-ENET-L 設定ツール 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
GT SoftGOT1000 Version3 全バージョン
GT SoftGOT2000 Version1 全バージョン
GX LogViewer 全バージョン
GX Works2 全バージョン
GX Works3 全バージョン
MELSOFT FieldDeviceConfigurator 全バージョン
MELSOFT iQ AppPortal 全バージョン
MELSOFT MaiLab 全バージョン
MELSOFT Navigator 全バージョン
MELSOFT Update Manager 全バージョン
MX Component 全バージョン
MX Sheet 全バージョン
PX Developer 全バージョン
RT ToolBox3 全バージョン
RT VisualBox 全バージョン
データ転送ツール 全バージョン
データ転送ツール Classic 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、デフォルト以外のインストールフォルダにインストールされている場合に、不適切なデフォルトパーミッション(CWE-276)により、悪意のあるプログラムが実行される脆弱性が存在します。該当製品が、デフォルトのインストールフォルダにインストールされている場合には、本脆弱性の影響を受けません。

■脆弱性がもたらす脅威
本脆弱性を悪意のある攻撃者に悪用された場合に、悪意のあるプログラムが実行され、情報を取得される、情報を改ざん・破壊・削除される、サービス停止(DoS)状態にされる等の可能性があります。

1 https://cwe.mitre.org/data/definitions/276.html
2 https://www.ipa.go.jp/security/vuln/CVSSv3.html

■お客様での対応
対策版のリリース予定はございませんので、軽減策・回避策にて対応をお願いいたします。

■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。
・デフォルトのインストールフォルダにインストールする。ただし、下記製品に限っては、必ず下記バージョン以降の製品を使用する(※)。
(※)下記バージョンより前の製品には、CVE-2020-14496[3]の脆弱性が存在し、軽減策の効果がありません。

製品名	バージョン
CPU ユニットロギング設定ツール	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
データ転送ツール	Ver. 3.41T

・インストールフォルダの変更が必要な場合には、管理者権限を持ったユーザのみに変更権限が与えられたフォルダを、インストールフォルダとして指定する。
・該当製品を使用するパソコンにウイルス対策ソフトを搭載する。
・該当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、ユーザからのリモートログインをブロックする。
・該当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。
・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
この問題をご報告いただいた、ZHEJIANG QIAN INFORMATION & TECHNOLOGY CO., LTD.の 01dGu0 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

■更新履歴
2024 年 7 月 4 日
・「該当製品の確認方法」に以下の製品を追加しました。
AL-PCS/WIN-E、CPU ユニットロギング設定ツール、EZSocket、FR Configurator2、FX Configurator-EN、FX Configurator-FP、FX3U-ENET-L 設定ツール、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、データ転送ツール、データ転送ツール Classic
・上記に伴い、「概要」、「脆弱性の説明」および「軽減策・回避策」を修正しました。

[3] https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2020-006.pdf