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 11 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、ファイル名やパス名の外部制御(CWE-73[1])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、細工したプロジェクトファイルをユーザに開かせることにより、悪意のあるプログラムを実行し、情報を窃取したり、情報を改ざん・破壊・削除したり、対象をサービス停止(DoS)状態に陥らせたりすることができる可能性があります(CVE-2023-5247)。
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-2023-5247　CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H 基本値:7.8

■該当製品の確認方法
影響を受ける製品は以下の製品です。
<製品とバージョン>

製品名	バージョン
GX Works3	全バージョン
MELSOFT iQ AppPortal	全バージョン
MELSOFT Navigator	全バージョン
モーション制御設定(*1)	全バージョン

(*1) GX Works3 に同梱されたソフトウェア

<バージョンの確認方法>
・GX Works3 ：「GX Works3 オペレーティングマニュアル」の「1.8 GX Works3 の操作方法について調べる」の「GX Works3 のバージョン確認」を参照ください。
・MELSOFT iQ AppPortal ：「iQ AppPortal オペレーティングマニュアル」の「1.4 iQ AppPortal の操作方法について調べる」の「iQ AppPortal のバージョン確認」を参照ください。
・MELSOFT Navigator ：「MELSOFT Navigator Version2 ヘルプ」の「2 画面構成と基本操作」の「9.3 MELSOFT Navigator のバージョン情報を確認する」を参照ください。
・モーション制御設定 ：「モーション制御設定機能ヘルプ」の「1.2 モーション制御設定機能の操作方法について調べる」の「モーション制御設定機能のバージョン確認」を参照ください。

■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、ファイル名やパス名の外部制御(CWE-73)に起因する、悪意のあるプログラムが実行される脆弱性(CVE-2023-5247)が存在します。

■脆弱性がもたらす脅威
攻撃者は、細工したプロジェクトファイルをユーザに開かせることにより、悪意のあるプログラムを実行し、情報を窃取したり、情報を改ざん・破壊・削除したり、対象をサービス停止(DoS)状態に陥らせたりすることができ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。

■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。
・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。

1 https://cwe.mitre.org/data/definitions/73.html
2 https://www.ipa.go.jp/security/vuln/CVSSv3.html

■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