複数の FA 製品における
悪意のあるコードが実行される脆弱性

公開日 2020 年 7 月 30 日
三菱電機株式会社

■概要
三菱電機製の複数の FA 製品において、パストラバーサルにより、悪意ある攻撃者に任意のコードを実行される脆弱性があります。
この脆弱性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。

■該当製品の確認方法
〈製品とバージョン〉
CW Configurator Ver. 1.010L 以前
FR Configurator2 Ver. 1.22Y 以前
GX Works2 Ver. 1.595V 以前
GX Works3 Ver. 1.063R 以前
IU Configuration Tool 全バージョン
IU Developer2 全バージョン
MELSEC iQ-R シリーズ モーションユニット 全バージョン
MELSOFT iQ AppPortal 全バージョン
MELSOFT Navigator 全バージョン
MI Configurator 全バージョン
MR Configurator2 全バージョン
MT Works2 Ver. 1.156N 以前
MX Component 全バージョン
RT ToolBox3 Ver. 1.70Y 以前

〈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
三菱電機製の複数の FA 製品において、パストラバーサル(CWE-22)により、悪意のある攻撃者に任意のコードが実行される脆弱性(CVE-2020-14523)が存在します。

■脆弱性がもたらす脅威
悪意ある攻撃者によって細工されたプロジェクトファイル/設定データファイルを、お客様が操作してしまうことにより、次のような影響を受ける可能性があります。

・操作しているお客様が管理者権限の場合、そのプロジェクトファイル/設定データファイルの作用により、実行ファイルや設定データファイルの書き換えが可能となる。結果として攻撃者は任意のコードに書き替え、実行することが可能となる。

■対策方法
以下サイトより各ソフトウェア製品の最新版をダウンロードしたうえで、アップデートしてください。
https://www.mitsubishielectric.co.jp/fa/download/index.html

対策済のソフトウェア製品およびバージョンは、以下となります。

〈製品とバージョン〉
CW Configurator Ver. 1.011M 以降
FR Configurator2 Ver. 1.23Z 以降
GX Works2 Ver. 1.596W 以降
GX Works3 Ver. 1.065T 以降
MT Works2 Ver. 1.160S 以降
RT ToolBox3 Ver. 1.80J 以降

〈アップデート方法〉
各製品のマニュアルまたはヘルプをご参照ください。

■回避策
対策バージョンがリリースされていない製品をお使いのお客様、あるいはすぐに製品をアップデート出来ないお客様に対し、これらの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。

・該当製品で使用するプロジェクトファイルや設定データファイルを、メール、USB メモリ、ファイルサーバなどで第三者から受け取る場合は、ファイルが正しい入手経路で取得されたものであることを確認する。(または、入手経路不明なファイルが混入してないことを確認する。)
・該当製品を管理者権限を持たないアカウントで操作する。(MELSEC iQ-R シリーズ モーションユニットは非該当。)
・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。(MELSEC iQ-R シリーズ モーションユニットは非該当。)
・すべての制御システムデバイスやシステムのネットワークへの接続を最小限に抑え、信頼できないネットワークやホストからアクセスできないようにする。
・制御システムネットワークとリモートデバイスをファイアウォールで防御し、OA ネットワークから分離する。
・リモートアクセスが必要な場合は、仮想プライベートネットワーク(VPN)を使用する。

■謝辞
この問題をご報告いただいた Claroty 社 Mashav Sapir 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。