

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 エンジニアリングソフトウェア製品において、悪意のあるコードが実行される脆弱性が存在します。本脆弱性を悪用された場合、情報を取得される、情報を改ざんされる、サービス運用妨害 (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。

■該当製品の確認方法

〈製品とバージョン〉

C 言語コントローラインタフェースユニットユーティリティ 全バージョン
C 言語コントローラ用設定・モニタツール 全バージョン
CC-Link IE コントローラネットワークデータコレクタ: パソコンボード用 全バージョン
CC-Link IE フィールドネットワークデータコレクタ: パソコンボード用 全バージョン
CPU ユニットロギング設定ツール Ver. 1.100E 以前
CW Configurator Ver. 1.010L 以前
データ転送ツール 全バージョン
EZSocket 全バージョン
FR Configurator SW3 全バージョン
FR Configurator2 全バージョン
GT Designer2 Classic 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 Developer Ver. 8.504A 以前
GX LogViewer Ver. 1.100E 以前
GX Works2 全バージョン
GX Works3 Ver. 1.063R 以前
IU Data Transfer 全バージョン
IU Developer 全バージョン
IU Developer2 全バージョン
M_CommDTM-IO-Link 全バージョン
MELFA-Works 全バージョン
WinCPU 設定ユーティリティ 全バージョン
MELSOFT 環境削除ツール 全バージョン
MELSOFT EM Software Development Kit 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
モーション制御設定 Ver. 1.005F 以前
Motorizer Ver. 1.005F 以前
MR Configurator2 全バージョン
MT Works2 全バージョン
MTConnect データコレクタ 全バージョン
MX Component 全バージョン
MX MESInterface 全バージョン
MX MESInterface-R 全バージョン
MX Sheet 全バージョン
ネットワークインタフェースボード CC IE Control ユーティリティ 全バージョン
ネットワークインタフェースボード CC IE Field ユーティリティ 全バージョン
ネットワークインタフェースボード CC-Link Ver.2 ユーティリティ 全バージョン
ネットワークインタフェースボード MNETH ユーティリティ 全バージョン
ポジションボードユーティリティ2 全バージョン
PX Developer 全バージョン
RT ToolBox2 全バージョン
RT ToolBox3 全バージョン
C 言語コントローラ設定・モニタツール 全バージョン

SLMP データコレクタ 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

三菱電機製の複数の FA エンジニアリングソフトウェア製品には、悪意のあるコードが実行される脆弱性(CVE-2020-14521)が存在します。これは製品の一部のファイルに不適切な権限が与えられており、悪意のある攻撃者によってこれらのファイルが悪意あるファイルに置き換えられる可能性がある(CWE-428)ことによります。

■脆弱性がもたらす脅威

この脆弱性を悪意ある攻撃者に利用された場合、情報を取得される、情報を改ざんされる、サービス運用妨害 (DoS)状態にされる等の可能性があります。

■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>

CPU ユニットロギング設定ツール Ver. 1.106K 以降

CW Configurator Ver. 1.011M 以降

GX Developer Ver. 8.505B 以降

GX LogViewer Ver. 1.106K 以降

GX Works3 Ver. 1.065T 以降

モーション制御設定 Ver. 1.006G 以降

Motorizer Ver. 1.010L 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。

・Windows を起動した際に「ファイル名に関する警告」メッセージが表示された場合は、ファイル名の変更等のメッセージの指示に従って適切な処置を行った後に、該当製品のインストールや操作を行なう。

・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。

・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。

・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。