複数の FA エンジニアリングソフトウェア製品における
不適切なファイルアクセス制御の脆弱性

公開日 2020 年 7 月 30 日
最終更新日 2022年9月22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、不適切なファイルアクセス制御の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、権限昇格と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。

■該当製品の確認方法

<該当製品とバージョン>
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 Ver. 3.40S 以前
EZSocket Ver. 4.5 以前
FR Configurator2 Ver. 1.22Y 以前
GT Designer3 Version1 (GOT2000) Ver. 1.235V 以前
GT SoftGOT1000 Version3 Ver. 3.200J 以前
GT SoftGOT2000 Version1 Ver. 1.235V 以前
GX LogViewer Ver. 1.100E 以前
GX Works2 Ver. 1.592S 以前
GX Works3 Ver. 1.063R 以前
M_CommDTM-HART Ver. 1.00A
M_CommDTM-IO-Link Ver. 1.03D 以前
MELFA-Works Ver. 4.3 以前
WinCPU 設定ユーティリティ Ver. 1.03D 以前
MELSOFT EM Software Development Kit (EM Configurator) Ver. 1.010L 以前
MELSOFT FieldDeviceConfigurator Ver. 1.03D 以前
MELSOFT Navigator Ver. 2.62Q 以前
MH11 SettingTool Version2 Ver. 2.002C 以前
MI Configurator Ver. 1.004E 以前
Motorizer Ver. 1.005F 以前
MR Configurator2 Ver. 1.105K 以前
MT Works2 Ver. 1.156N 以前
MX Component Ver. 4.19V 以前
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 Ver. 1.29F 以前
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 Ver. 1.16S 以前
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 Ver. 1.23Z 以前
ネットワークインタフェースボード MNETH ユーティリティ Ver. 34L 以前
PX Developer Ver. 1.52E 以前
RT ToolBox2 Ver. 3.72A 以前
RT ToolBox3 Ver. 1.70Y 以前
C 言語コントローラ設定・モニタツール (SW4PVC-CCPU) Ver. 4.12N 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 エンジニアリングソフトウェア製品において、製品の一部のファイルに不適切な権限が与えられる(CWE-275)ため、悪意のある攻撃者によって細工されたファイルに置き換えられる脆弱性があります(CVE-2020-14496)。管理者権限をもったユーザが置き換えられたファイルを実行することにより、情報を取得される、情報を改ざん・破壊される、サービス停止(DoS)状態にされる等の可能性があります。

■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、権限昇格と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。

■対策方法
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
データ転送ツール Ver. 3.41T 以降
EZSocket Ver. 4.6 以降 (*1)
FR Configurator2 Ver. 1.23Z 以降
GT Designer3 Version1 (GOT2000) Ver. 1.236W 以降
GT SoftGOT1000 Version3 Ver.3.245F 以降
GT SoftGOT2000 Version1 Ver. 1.236W 以降
GX LogViewer Ver. 1.106K 以降
GX Works2 Ver. 1.595V 以降
GX Works3 Ver. 1.065T 以降
M_CommDTM-HART Ver. 1.01B 以降
M_CommDTM-IO-Link Ver. 1.04E 以降
MELFA-Works Ver. 4.4 以降
MELSOFT EM Software Development Kit (EM Configurator) Ver. 1.015R 以降
MELSOFT FieldDeviceConfigurator Ver. 1.04E 以降
MELSOFT Navigator Ver. 2.70Y 以降
MH11 SettingTool Version2 Ver. 2.003D 以降
MI Configurator Ver. 1.005F 以降
Motorizer Ver. 1.010L 以降
MR Configurator2 Ver. 1.106L 以降
MT Works2 Ver. 1.160S 以降
MX Component Ver. 4.20W 以降
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 Ver. 1.30G 以降
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 Ver. 1.17T 以降
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 Ver. 1.24A 以降
ネットワークインタフェースボード MNETH ユーティリティ Ver. 35M 以降
PX Developer Ver. 1.53F 以降
RT ToolBox2 Ver. 3.73B 以降
RT ToolBox3 Ver. 1.80J 以降
C 言語コントローラ設定・モニタツール (SW4PVC-CCPU) Ver. 4.13P 以降

WinCPU 設定ユーティリティ(MELSEC-Q シリーズ WinCPU ユニット用の設定ツール)については対策版リリースがございませんので、後継機種となります MELSEC iQ-R シリーズ WinCPU ユニットへの移行および設定ツール CW Configurator(SW1DND-RCCPU-J)の使用を推奨いたします。

<対策品の入手方法>
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(*1 の製品を除く)。
https://www.mitsubishielectric.co.jp/fa/download/index.html

(*1) EZSocket は三菱電機パートナー企業向けの通信ミドルウェア製品です。対策品は三菱電機よりパートナー企業に直接提供してまいります。

<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。

■軽減策・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。

・該当製品をインストールしているパソコンに、対策バージョンの GX Works3、GX Works2 または MELSOFT Navigator をインストールする。これは、これら3つの製品が、同じフォルダ(例:C:¥Program files¥MELSOFT)にインストールされた他製品に対しても、同じ対策効果を与える包括的な対策を提供するためである。
・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。
・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 Nozomi Networks 社 Younes Dragoni 様、Applied Risk 社 research team 様、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。

■更新履歴

2022 年 9 月 22 日

以下の機種の対策方法の情報を追加しました。

WinCPU 設定ユーティリティ

2022 年 7 月 28 日

以下の機種の対策方法の情報を追加しました。

MI Configurator、C 言語コントローラ設定・モニタツール (SW4PVC-CCPU)

C 言語コントローラ設定・モニタツール (SW3PVC-CCPU)を該当製品から削除しました。

2022 年 5 月 24 日

以下の機種の対策方法の情報を追加しました。

M_CommDTM-IO-Link、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、
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、
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、ネットワークインタフェースボード MNETH ユーティリティ

2020 年 12 月 17 日

GT SoftGOT1000 Version3 の対策方法の情報を追加しました。