複数の FA エンジニアリングソフトウェア製品における
複数のサービス拒否(DoS)の脆弱性

公開日 2021 年 2 月 18 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、複数のサービス拒否(DoS)の脆弱性が存在することが判明しました。攻撃者が細工したパケットを送信し、当該ソフトウェア製品が受信すると、当該ソフトウェア製品がサービス拒否(DoS)状態に陥る可能性があります。(CVE-2021-20587、CVE-2021-20588)

■CVSS スコア

CVE-2021-20587: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H 基本値:7.5
CVE-2021-20588: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H 基本値:7.5

■該当する製品の確認方法

<製品とバージョン>

・C 言語コントローラ用設定・モニタツール (*1) 全バージョン
・CPU ユニットロギング設定ツール (*1) 全バージョン
・CW Configurator (*1) 全バージョン
・データ転送ツール (*1) 全バージョン
・EZSocket (*1)(*2)(*3) 全バージョン
・FR Configurator (*2) 全バージョン
・FR Configurator SW3 (*2) 全バージョン
・FR Configurator2 (*2) 全バージョン
・GT Designer3 Version1(GOT1000) (*3) 全バージョン
・GT Designer3 Version1(GOT2000) (*3) 全バージョン
・GT SoftGOT1000 Version3 (*3) 全バージョン
・GT SoftGOT2000 Version1 (*3) 全バージョン
・GX Configurator-DP (*1) 7.14Q 以前
・GX Configurator-QP (*1) 全バージョン
・GX Developer (*1) 全バージョン
・GX Explorer (*1) 全バージョン
・GX IEC Developer (*1) 全バージョン
・GX LogViewer (*1) 全バージョン
・GX RemoteService-I (*1) 全バージョン
・GX Works2 (*1) 1.597X 以前
・GX Works3 (*1) 1.070Y 以前
・M_CommDTM-HART (*1) 全バージョン
・M_CommDTM-IO-Link (*1) 全バージョン
・MELFA-Works (*1) 全バージョン
・WinCPU 設定ユーティリティ (*1) 全バージョン
・MELSOFT EM Software Development Kit (EM Configurator) (*1) 全バージョン
・MELSOFT Navigator (*1)(*2)(*3) 全バージョン
・MH11 SettingTool Version2 (*1) 全バージョン
・MI Configurator (*1) 全バージョン
・MT Works2 (*1) 全バージョン
・MX Component (*1)(*2)(*3) 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 (*1) 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 (*1) 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 (*1) 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 (*1) 全バージョン
・PX Developer (*1) 全バージョン
・RT ToolBox2 (*1) 全バージョン
・RT ToolBox3 (*1) 全バージョン
・C 言語コントローラ設定・モニタツール (*1) 全バージョン
・SLMP データコレクタ (*1) 全バージョン

(*1) 三菱電機製シーケンサ製品と通信を行うソフトウェア製品。
(*2) 三菱電機製インバータ製品と通信を行うソフトウェア製品。
(*3) 三菱電機製 GOT 製品と通信を行うソフトウェア製品。

〈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以下に示す複数の脆弱性が存在するため、悪意ある第三者の攻撃により、当該ソフトウェア製品がサービス拒否(DoS)状態に陥る可能性があります。

・ヒープベースのバッファオーバーフロー(CWE-122): CVE-2021-20587
・長さパラメータの不整合時の不適切な取り扱い(CWE-130): CVE-2021-20588

■脆弱性がもたらす脅威
攻撃者が、三菱電機製シーケンサ、GOT、あるいはインバータ製品になりすまして一部細工した応答パケットを返信し、当該ソフトウェア製品に受信させることにより、当該ソフトウェア製品をサービス拒否(DoS)状態に陥らせる可能性があります。また、確認されておりませんが、悪意のあるプログラムが実行される可能性もあります。

■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〉
・GX Configurator-DP 7.15R 以降
・GX Works2 1.600A 以降
・GX Works3 1.072A 以降

〈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。
https://www.mitsubishielectric.co.jp/fa/download/index.html

〈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て、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。

・三菱電機製シーケンサと通信を行うソフトウェア製品の場合(*4)、該当の製品をインストールしているパソコンに、対策済の GX Works3 をインストールする(GX Works3 の対策品が、同じパソコン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)。
・該当の製品を管理者権限を持たないアカウントで操作する。
・該当の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。

(*4) 三菱電機製インバータ製品、GOT 製品との通信における対策用ソフトウェア製品は現在開発中です。

■謝辞
この問題をご報告いただいた dliangfun 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