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
最終更新日 2022 年 11 月 17 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>

・CPU ユニットロギング設定ツール (*1) Ver. 1.112R 以前
・CW Configurator (*1) Ver. 1.011M 以前
・データ転送ツール (*3) Ver. 3.44W 以前
・EZSocket (*1)(*2)(*3) Ver. 5.4 以前
・FR Configurator (*2) 全バージョン
・FR Configurator SW3 (*2) 全バージョン
・FR Configurator2 (*2) Ver. 1.24A 以前
・GT Designer3 Version1(GOT1000) (*3) Ver. 1.250L 以前
・GT Designer3 Version1(GOT2000) (*3) Ver. 1.250L 以前
・GT SoftGOT1000 Version3 (*3) Ver. 3.245F 以前
・GT SoftGOT2000 Version1 (*3) Ver. 1.250L 以前
・GX Configurator-DP (*1) Ver. 7.14Q 以前
・GX Configurator-QP (*1) 全バージョン
・GX Developer (*1) Ver. 8.506C 以前
・GX Explorer (*1) 全バージョン
・GX IEC Developer (*1) 全バージョン
・GX LogViewer (*1) Ver. 1.115U 以前
・GX RemoteService-I (*1) 全バージョン
・GX Works2 (*1) Ver. 1.597X 以前
・GX Works3 (*1) Ver. 1.070Y 以前
・iQMonozukuri アンドン (データ転送ツール(*3)) 全バージョン
・iQMonozukuri 工程リモート監視 (データ転送ツール(*3)) 全バージョン
・M_CommDTM-HART (*1) 全バージョン
・M_CommDTM-IO-Link (*1) Ver. 1.03D 以前
・MELFA-Works (*1) Ver. 4.4 以前
・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) 1.015R 以前
・MELSOFT Navigator (*1)(*2)(*3) Ver. 2.74C 以前
・MH11 SettingTool Version2 (*1) Ver. 2.004E 以前
・MI Configurator (*1) Ver. 1.004E 以前
・MT Works2 (*1) Ver. 1.167Z 以前
・MX Component (*1)(*2)(*3) Ver. 5.001B 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 (*1) 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 (*1) 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 (*1) 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 (*1) Ver. 34L 以前
・PX Developer (*1) Ver. 1.53F 以前
・RT ToolBox2 (*1) Ver. 3.73B 以前
・RT ToolBox3 (*1) Ver. 1.82L 以前
・C 言語コントローラ設定・モニタツール (SW4PVC-CCPU) (*1) Ver. 4.12N 以前
・SLMP データコレクタ (*1) Ver. 1.04E 以前

(*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〉
・CPU ユニットロギング設定ツール Ver. 1.118X 以降
・CW Configurator Ver. 1.012N 以降
・データ転送ツール Ver. 3.45X 以降(*4)
・EZSocket Ver. 5.5 以降(*5)
・FR Configurator2 Ver. 1.25B 以降
・GT Designer3 Version1（GOT1000） Ver. 1.255R 以降
・GT Designer3 Version1（GOT2000） Ver. 1.255R 以降
・GT SoftGOT1000 Version3 Ver. 3.255R 以降
・GT SoftGOT2000 Version1 Ver. 1.255R 以降
・GX Configurator-DP Ver. 7.15R 以降(*6)
・GX Developer Ver. 8.507D 以降
・GX LogViewer Ver. 1.118X 以降
・GX Works2 Ver. 1.600A 以降
・GX Works3 Ver. 1.072A 以降
・M_CommDTM-IO-Link Ver. 1.04E 以降
・MELFA-Works Ver. 4.5 以降
・MELSOFT EM Software Development Kit (EM Configurator) Ver.1.020W 以降
・MELSOFT Navigator Ver. 2.78G 以降
・MH11 SettingTool Version2 Ver. 2.005F 以降
・MI Configurator Ver. 1.005F 以降
・MT Works2 Ver. 1.170C 以降
・MX Component Ver. 5.002C 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. 1.54G 以降
・RT ToolBox2 Ver. 3.74C 以降
・RT ToolBox3 Ver. 1.90U 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
・SLMP データコレクタ Ver. 1.05F 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。

(*4) iQ Monozukuri アンドン及び iQ Monozukuri 工程リモート監視は、データ転送ツールの最新版をダウンロードしアップデートの上ご利用ください。
(*5) EZSocket の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。
(*6) GX Configurator-DP に関しては、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。

■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、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）。
・三菱電機製インバータと通信を行うソフトウェア製品の場合、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 FR Configurator2 をインストールする（FR Configurator2 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）。
・GOT 製品と通信を行うソフトウェア製品の場合、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 GT Designer3 をインストールする（GT Designer3 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。

■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

■更新履歴
2022 年 11 月 17 日
影響を受ける製品において、下記の製品の対策方法の情報を追加
MELSOFT EM Software Development Kit (EM Configurator)

2022 年 7 月 28 日
影響を受ける製品において、下記の製品の対策方法の情報を追加
EZSocket、MI Configurator、C 言語コントローラ設定・モニタツール (SW4PVC-CCPU)
影響を受ける製品から、C 言語コントローラ設定・モニタツール (SW3PVC-CCPU)を削除

2022 年 5 月 24 日
影響を受ける製品において、下記の製品の対策方法の情報を追加
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

2022 年 2 月 8 日
影響を受ける製品において、下記の製品の対策方法の情報を追加
MT Works2、MX Component、SLMP データコレクタ

2021 年 11 月 16 日
影響を受ける製品において、下記の製品の対策方法の情報を追加
MELFA-Works、MH11 SettingTool Version2、RT ToolBox2

2021 年 7 月 27 日
影響を受ける製品において、下記の製品の対策方法の情報を追加
GX Developer、MELSOFT Navigator

2021 年 5 月 27 日
影響を受ける製品において、下記の製品の対策方法の情報を追加
CPU ユニットロギング設定ツール、CW Configurator、データ転送ツール、FR Configurator2、
GT Designer3 Version1（GOT1000）、GT Designer3 Version1（GOT2000）、GT SoftGOT1000 Version3、
GT SoftGOT2000 Version1、GX LogViewer、PX Developer、RT ToolBox3
影響を受ける製品を追加
iQMonozukuri アンドン （データ転送ツール）、iQMonozukuri 工程リモート監視 （データ転送ツール）