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 12 月 16 日
最終更新日 2022 年 7 月 28 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。攻撃者により改ざんされたプロジェクトファイル(*1)を当該ソフトウェア製品で開くと、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-2021-20606、CVE-2021-20607)

(*1) ソフトウェア製品で作成するデータファイル。

■CVSS スコア
CVE-2021-20606: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H 基本値:5.5
CVE-2021-20607: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H 基本値:5.5

■該当製品の確認方法
<製品とバージョン>
・GX Works2 Ver. 1.606G 以前
・MELSOFT Navigator Ver. 2.84N 以前
・EZSocket Ver. 5.4 以前(*2)

<バージョンの確認方法>
・GX Works2: 「GX Works2 Version1 オペレーティングマニュアル(共通編)」の「3.4.4 GX Works2 のバージョンを確認する」を参照ください。
・MELSOFT Navigator: 「MELSOFT Navigator Version2 ヘルプ」の「8.3 MELSOFT Navigator のバージョン情報を確認する」を参照ください。

(*2) 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。バージョンの確認方法は三菱電機よりパートナー企業に直接ご連絡します。

■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。

・CVE-2021-20606: 境界外読み取り(CWE-125)
・CVE-2021-20607: 整数アンダーフロー(CWE-191)

■脆弱性がもたらす脅威
攻撃者により改ざんされたプロジェクトファイルを当該ソフトウェア製品で開くと、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。

■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 Works2 Ver. 1.610L 以降
・MELSOFT Navigator Ver. 2.86Q 以降
・EZSocket Ver. 5.5 以降(*3)

<対策品の入手方法>
以下サイトより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>
1. ダウンロードしたファイル(zip 形式)を解凍します。
2. 解凍されたフォルダ中の setup.exe を実行してインストールを行ってください。

(*3) 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。

■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。

・コンピュータ/サーバ内のプロジェクトファイルが悪意ある第三者に改ざんされないように、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。
・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。
・信頼できない発信者からのメール等で送付されたプロジェクトファイルを開かない。
・MELSOFT Navigator 又は EZSocket の一括読出し機能で読み出した GX Works2 のプロジェクトファイルに対しては、以下を実行する。

1. MELSOFT Navigator 又は EZSocket で読み出した GX Works2 のプロジェクトファイルを GX Works2 1.610L 以降で開きます。
2. GX Works2 のツールーオプションの「プロジェクト」-「共通設定」内の項目「プロジェクトのセキュリティチェックを有効にする」を有効にして保存を実行してください。

■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 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

2022 年 6 月 30 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 Navigator