GX Works2 におけるサービス拒否(DoS)の脆弱性

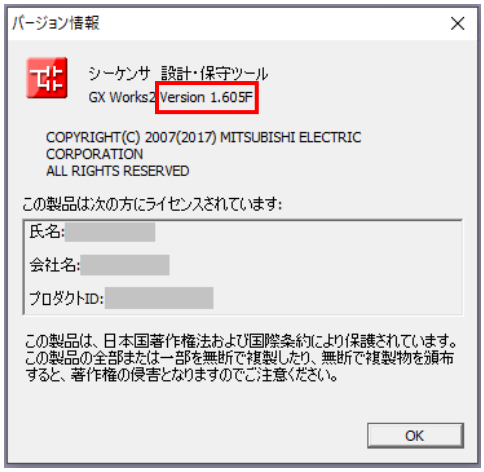
公開日 2021 年 12 月 16 日
三菱電機株式会社

■概要
三菱電機製の FA エンジニアリングソフトウェア製品 GX Works2 において、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。攻撃者により不正なパケットを三菱電機製シーケンサへ送信されることによって改ざんされたシーケンサ内のプログラムファイルを、GX Works2 が読み出すと、GX Works2 がサービス拒否(DoS)状態に陥る可能性があります。(CVE-2021-20608)

■CVSS スコア
CVE-2021-20608: CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H 基本値:5.3

■該当製品の確認方法
影響を受ける製品およびバージョンは以下の通りです。
・GX Works2 Ver.1.606G 以前

<バージョンの確認方法>
1. GX Works2 を実行します。
2. メニューの[ヘルプ] -> [バージョン情報]を選択します。
3. [バージョン情報]画面が表示されるので、バージョンを確認します。



■脆弱性の説明
三菱電機製 GX Works2 において、長さパラメータの不整合時の不適切な取り扱い(CWE-130)により、サービス拒否(DoS)の脆弱性が存在します。

■脆弱性がもたらす脅威
攻撃者により不正なパケットを三菱電機製シーケンサへ送信されることによって改ざんされたシーケンサ内のプログラムファイルを、GX Works2 が読み出すと、GX Works2 がサービス拒否(DoS)状態に陥る可能性があります。
本脆弱性によるシーケンサの誤動作はありません。

■対策方法
以下サイトより Ver.1.610L 以降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の中の「setup.exe」を実行してインストールを行ってください。

■回避策
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。

・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。
・三菱電機製シーケンサへの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。

■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