GX Works2 のシミュレーション機能における
サービス拒否(DoS)の脆弱性

公開日 2023 年 11 月 21 日
三菱電機株式会社

■概要
GX Works2 のシミュレーション機能において、不適切な入力確認(CWE-20[1])によるサービス拒否(DoS)の脆弱性が存在することが判明しました。攻撃者は、該当機能に対して不正なパケットを送信することにより、当該機能をサービス停止(DoS)状態に陥らせることができる可能性があります(CVE-2023-5274、CVE-2023-5275)。ただし、攻撃者は、当該機能が動作する同一 PC 内からパケットを送信する必要があります。

■CVSS スコア [2]
CVE-2023-5274　CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L 基本値:2.5
CVE-2023-5275　CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L 基本値:2.5

■該当製品の確認方法
影響を受ける製品は以下の製品です。
<製品とバージョン>
GX Works2 全バージョン

<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 ヘルプ」の「3.4.4 GX Works2 のバージョンを確認する」を参照ください。

■脆弱性の説明
GX Works2 のシミュレーション機能には、不適切な入力確認（CWE-20）によるサービス拒否(DoS)の脆弱性(CVE-2023-5274、CVE-2023-5275)が存在します。

■脆弱性がもたらす脅威
攻撃者は、GX Works2 のシミュレーション機能に対して不正なパケットを送信することにより、当該機能をサービス停止(DoS)状態に陥らせることができる可能性があります。ただし、攻撃者は、当該機能が動作する同一の PC 内からパケットを送信する必要があります。

■対策方法
軽減策・回避策にて対応をお願いいたします。

■軽減策・回避策
本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。
・該当製品を使用する PC にウイルス対策ソフトを搭載してください。
・該当製品を使用する PC を LAN 内で使用し、信頼できないネットワークやホスト、ユーザからのリモートログインをブロックしてください。
・該当製品をインストールされた PC をインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク（VPN)等で不正アクセスを防止したうえで、信頼できるユーザのみにリモートログインを許可してください。
・信頼できないファイルを開いたり、信頼できないリンクをクリックしないでください。

■謝辞
この問題をご報告いただいた、ZheJiangQiAnTechnology の joker63 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

1 https://cwe.mitre.org/data/definitions/20.html
2 https://www.ipa.go.jp/security/vuln/CVSSv3.html