GX Works2 における情報漏えいの脆弱性

公開日 2025 年 11 月 27 日
三菱電機株式会社

■概要
GX Works2 において、情報漏えいの脆弱性が存在することが判明しました。GX Works2 は認証情報を平文で保存しており、攻撃者は、平文で保存された認証情報をプロジェクトファイルから取得することができます。結果として、取得された認証情報を用いて、ユーザ認証が設定されているプロジェクトファイルを開かれ、プロジェクトの情報を閲覧又は編集される可能性があります。(CVE-2025-3784)

■CVSS スコア [1]
CVE-2025-3784　CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N　基本値:5.5

■該当製品の確認方法
GX Works2 の全てのバージョンが該当します。

■脆弱性の説明
GX Works2 には、重要な情報の平文保存(CWE-312[2])に起因する情報漏えいの脆弱性が存在します。

■脆弱性がもたらす脅威
攻撃者は、平文で保存された認証情報をプロジェクトファイルから取得することができます。結果として、取得された認証情報を用いて、ユーザ認証が設定されているプロジェクトファイルを開かれ、プロジェクトの情報を閲覧又は編集される可能性があります。

■お客様での対応
本脆弱性に対する対策を含むバージョンを、現在開発中です。
対策バージョンのリリースまでの間は、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。
・該当製品がインストールされた 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。
・該当製品が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。
・該当製品がインストールされた PC 並びに同 PC と通信可能な PC 及びネットワーク機器への物理的なアクセスを制限してください。
・該当製品を使用する PC にウィルス対策ソフトを搭載してください。
・プロジェクトファイルをインターネット経由で送受信する場合は、プロジェクトファイルを暗号化してください。

■謝辞
この脆弱性をご報告いただいた、Jiho Shin 氏(M.S. graduate, Sungkyunkwan University)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://www.ipa.go.jp/security/vuln/CVSSv3.html
2 https://cwe.mitre.org/data/definitions/312.html