GX Works3 及びモーション制御設定における
パスワード認証回避の脆弱性

公開日 2026 年 9 月 17 日
三菱電機株式会社

■概要
GX Works3 及びモーション制御設定のブロックパスワード設定機能において、認証アルゴリズムの不適切な実装(CWE-303[1])による、認証回避の脆弱性が存在することが判明しました。ローカルログイン可能な攻撃者は、当該製品を実行し、メモリ上の実行モジュールの一部を書き換えることにより、不適切なブロックパスワードであっても認証を成功させ制御プログラムを、不正に閲覧したり、改ざん・破壊・削除したりすることができる可能性があります(CVE-2026-15688)。
この問題の影響を受けるソフトウェア製品名およびバージョンを以下に示します。

■CVSS スコア [2]
CVE-2026-15688 CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:N/SC:N/SI:H/SA:H 基本値:9.2

■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>

製品名	バージョン
GX Works3	全バージョン
モーション制御設定(*1)	全バージョン

(*1) GX Works3 に同梱されたソフトウェア

<バージョンの確認方法>
・GX Works3 ： 「GX Works3 オペレーティングマニュアル」の「1.9 GX Works3 の操作方法について調べる」の「GX Works3 のバージョン確認」を参照ください。マニュアルは GX Works3 に同梱されている「e-Manual Viewer」にて閲覧可能です。
・モーション制御設定 ： 「モーション制御設定機能ヘルプ」の「1.2 モーション制御設定機能の操作方法について調べる」の「モーション制御設定機能のバージョン確認」を参照ください。

■脆弱性の説明
GX Works3 及びモーション制御設定のブロックパスワード設定機能において、認証アルゴリズムの不適切な実装(CWE-303)による、認証回避の脆弱性(CVE-2026-15688)が存在します。

■脆弱性がもたらす脅威
ローカルログイン可能な攻撃者は、当該製品を実行し、メモリ上の実行モジュールの一部を書き換えることにより、不適切なブロックパスワードであっても認証を成功させ制御プログラムを、不正に閲覧したり、改ざん・破壊・削除したりすることができる可能性があります。

■お客様での対応
回避策・軽減策にてご対応ください。

■回避策・軽減策
製品ごとの回避策を、下表に示します。

No.	製品名	回避策
1	GX Works3	Ver.1.096A 以降にアップデートし、プロジェクトのセキュリティバージョンを「2」に設定してください。詳細は、「GX Works3 オペレーティングマニュアル」の「15.9 データの不正な閲覧/改ざんの防止(セキュリティバージョン)」を参照して下さい。
2	モーション制御設定	Ver.1.070Y 以降にアップデートし、プロジェクトのセキュリティバージョンを「2」に設定してください。詳細は、「モーション制御設定機能ヘルプ」の「12.5 データの不正な閲覧/改ざんの防止(セキュリティバージョン)」を参照してください。また、本表 No.1 GX Works3 の回避方法を実施してください。

1 https://cwe.mitre.org/data/definitions/303.html
2 https://www.first.org/cvss/v4.0/specification-document

製品ごとのアップデート用ソフトウェアの入手先およびインストール方法を下表に示します。

No	製品名	入手先	インストール方法
1	GX Works3	https://www.mitsubishielectric.co.jp/fa/download/software/detailsearch.page?mode=software&kisyu=/plcr&shiryoid=0000000016&kisyuid=0&lang=0&select=0&softid=0&infostatus=0_0_0&viewradio=0&viewstatus=0&viewpos=0	入手先に記載の「インストール方法」に従ってインストールをしてください
2	モーション制御設定	https://www.mitsubishielectric.co.jp/fa/download/software/detailsearch.page?mode=software&kisyu=/ssc&shiryoid=0000000105&lang=1&select=0&softid=1&infostatus=1_8_1&viewradio=0	

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パソコンを 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。
・該当製品を使用するパソコン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。
・信頼できない送信元からのメール等に記載された Web リンクをクリックしないようにしてください。また、信頼できない電子メールの添付ファイルを開かないようにしてください。
・該当製品を使用するパソコンにウイルス対策ソフトを搭載してください。
・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。

■謝辞
本脆弱性をご報告いただいた、Mayeul Fargier 様、Erwan Cordier 様、Noé Flatreaud 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