MELSEC iQ-R シリーズ安全 CPU 及び SIL2 プロセス CPU ユニットにおける情報漏えいの脆弱性

公開日 2024 年 2 月 13 日
三菱電機株式会社

■概要
MELSEC iQ-R シリーズ安全 CPU 及び SIL2 プロセス CPU ユニットには、不適切な権限設定(CWE-266)[1]による情報漏えいの脆弱性が存在することが判明しました。攻撃者が、当該 CPU ユニットに対して、管理者以外のユーザでログインした後に、細工したパケットを送信することにより、自分より低いアクセスレベルのユーザの認証情報(ユーザ ID 及びパスワード)を窃取できる可能性があります。(CVE-2023-6815)

■CVSS スコア [2]
CVE-2023-6815 CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N 基本値:6.5

■該当製品の確認方法
影響を受ける製品の形名とバージョンは以下のとおりです。

シリーズ	形名	ファームウェアバージョン
MELSEC iQ-R シリーズ安全 CPU	R08/16/32/120SFCPU	全バージョン
MELSEC iQ-R シリーズ SIL2 プロセス CPU	R08/16/32/120PSFCPU	全バージョン

■脆弱性の説明
MELSEC iQ-R シリーズ安全 CPU 及び SIL2 プロセス CPU ユニットには、不適切な権限設定(CWE-266)によ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
攻撃者が、当該 CPU ユニットに対して、管理者以外のユーザでログインした後に、細工したパケットを送信することにより、自分より低いアクセスレベルのユーザの認証情報(ユーザ ID 及びパスワード)を窃取できる可能性があります。

■対策方法
以下に示す回避策にて対応をお願いいたします。

■回避策
MELSEC iQ-R シリーズ安全 CPU ユニットでは、以下のバージョンの組合せにおいて、CPU ユニットへのユーザ情報書き込み時に「脆弱性対策強化バージョンの GX Works3 とのみ交信を行う」設定を有効とする(図 1 参照)ことで、本攻撃を防ぐことが可能です。
他ユニットでは、近日中に対応予定です。

シリーズ	CPU ユニットのバージョン	GX Works3 のバージョン
MELSEC iQ-R シリーズ安全 CPU	ファームウェアバージョン"27"以降	Version 1.087R 以降

上記バージョン以降の CPU ユニットへの変更については、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。

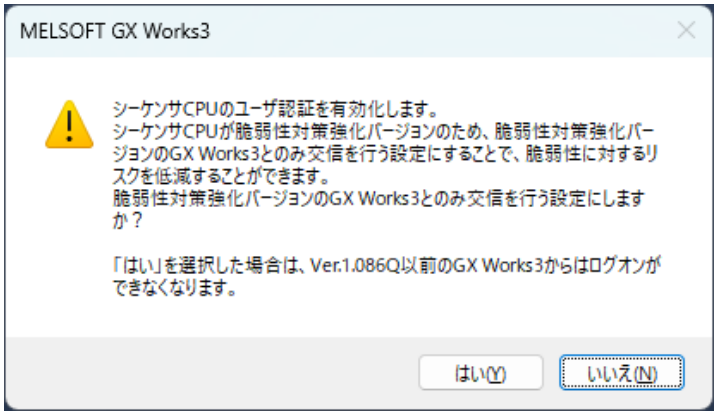

図 1 ユーザ情報書き込み時の選択画面

1 https://cwe.mitre.org/data/definitions/266.html
2 https://www.ipa.go.jp/security/vuln/CVSSv3.html

■軽減策

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。

・当該製品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)等を使用し、不正アクセスを防止してください。

・当該製品を LAN 内で使用し、信頼できないネットワークやホストからのアクセスをファイアウォールでブロックしてください。

・IP フィルタ機能※1 を使用し、信頼できないホストからのアクセスをブロックしてください。

※1： IP フィルタ機能については、以下の各製品のマニュアルを参照ください。

MELSEC iQ-R Ethernet ユーザーズマニュアル(応用編)の 1.13 セキュリティの「IP フィルタ」

・当該製品並びに当該製品へ接続可能なパソコン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。

・当該製品へアクセス可能なパソコンにウィルス対策ソフトを搭載してください。

■謝辞

この問題をご報告いただいた Dragos 社 Reid Wightman 様に感謝いたします。

■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