

MELSEC iQ-R シリーズ CPU ユニットにおける情報漏えいの脆弱性

公開日 2021 年 8 月 5 日
最終更新日 2024 年 4 月 18 日
三菱電機株式会社

■概要

MELSEC iQ-R シリーズ CPU ユニットには、ユーザ名に対する総当たり攻撃による情報漏えいの脆弱性(CWE-200)が存在することが判明しました。攻撃者は総当たり攻撃により、CPU ユニット内に格納される正規ユーザ名を窃取できる可能性があります。(CVE-2021-20594)

この脆弱性の影響を受ける製品形名およびファームウェアバージョンを以下に示します。

■CVSS スコア

CVE-2021-20594 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N 基本値:5.9

■該当製品の確認方法

次の製品形名とファームウェアバージョンのものが影響を受けます。

製品名	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	ファームウェアバージョン"26"以前
MELSEC iQ-R シリーズ SIL2 プロセス CPU	R08/16/32/120PSFCPU	ファームウェアバージョン"11"以前

ファームウェアバージョンの確認方法は、以下のマニュアルを参照ください。

・MELSEC iQ-R ユニット構成マニュアル「付 1 製造情報・ファームウェアバージョン」
マニュアルは以下サイトよりダウンロードが可能です。

<https://www.mitsubishielectric.co.jp/fa/download/index.html>

■脆弱性の説明

MELSEC iQ-R シリーズ CPU ユニットには、ユーザ名に対する総当たり攻撃による情報漏えいの脆弱性(CWE-200)が存在します。

■脆弱性がもたらす脅威

攻撃者によって、CPU ユニット内に格納される正規ユーザ名が窃取される可能性があります。ただし、CPU ユニットへのログインにはパスワードも必要なため、ユーザ名が窃取された場合でも、CPU ユニットへのログインは、容易ではありません。

■お客様での対応

該当製品・該当バージョンをご使用のお客様は、軽減策・回避策にて対応ください。

下記の通り対策済み製品をリリースしておりますが、対策版へのアップデートは出来ません。

■製品での対応

対策済の製品およびバージョンは、以下となります。

製品名	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	ファームウェアバージョン"27"以降
MELSEC iQ-R シリーズ SIL2 プロセス CPU	R08/16/32/120PSFCPU	ファームウェアバージョン"12"以降

■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。

- ・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、接続可能な IP アドレスを適切に制限してください。

※1: MELSEC iQ-R Ethernet ユーザーズマニュアル(応用編) セキュリティの「IP フィルタ」を参照ください。

■謝辞

この問題をご報告いただいた Nozomi NetworksLabs Ivan Speziale 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>

■更新履歴

2024年4月18日

ファームウェアバージョンの確認方法を追加しました。

「対策方法」を「お客様での対応」と「製品での対応」に分けました。

「製品での対応」に対応済みの製品を追加しました。

R08/16/32/120PSFCPU

2022年10月13日

「対策方法」に対応済みの製品を追加しました。

R08/16/32/120SFCPU