

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
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。

形名	ファームウェアバージョン
R08/16/32/120SFCPU	全バージョン
R08/16/32/120PSFCPU	全バージョン

■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。

■対策方法

近日中に、本脆弱性に対応したファームウェアを公開予定です。

■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。

- ・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>