MELSEC iQ-R シリーズ安全 CPU/SIL2 プロセス CPU ユニットにおける認証回避の脆弱性

公開日 2021 年 8 月 6 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 シリーズ安全 CPU/SIL2 プロセス CPU ユニットには、重要な情報の平文での送信（CWE-319[1]）の脆弱性が存在することが判明しました。攻撃者は、パスワード以外の認証情報を入手することにより、入手した認証情報を用いて、CPU ユニットへ不正にログインできる可能性があります。（CVE-2021-20599）

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 [2]

CVE-2021-20599　CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N 基本値: 9.1

■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 シリーズ安全 CPU/SIL2 プロセス CPU ユニットには、重要な情報の平文での送信の脆弱性が存在します。

■脆弱性がもたらす脅威

攻撃者が、パスワード以外の認証情報を入手することにより、入手した認証情報を用いて、CPU ユニットへ不正にログインできる可能性があります。

■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

対策済みのバージョンは、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 Networks の 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

1 https://cwe.mitre.org/data/definitions/319.html
2 https://www.ipa.go.jp/security/vuln/CVSSv3.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
・脆弱性タイプ(CWE)を重要な情報の平文での送信(CWE-319)に変更しました。

2021 年 10 月 12 日

・CVE 番号、および CVSS スコアを追加しました。
・概要、脆弱性の説明、脆弱性がもたらす脅威の内容を更新しました。