MELSEC シリーズ CPU ユニットの Web サーバ機能における サービス拒否(DoS)の脆弱性

公開日 2023 年 11 月 2 日
最終更新日 2024 年 2 月 15 日
三菱電機株式会社

■概要

MELSEC iQ-F/iQ-R シリーズの CPU ユニットの Web サーバ機能において、サービス拒否(DoS)の脆弱性が存在することが判明しました。攻撃者が連続して不正に Web サーバ機能へのログインを試行することにより、攻撃者による不正なログイン試行後ある一定期間が経過するまで、正規ユーザによる Web サーバ機能へのログインができなくなる可能性があります。攻撃者による不正なログイン試行が続く限り、本脆弱性の影響が続きます。(CVE-2023-4625)

■CVSS スコア [1]

CVE-2023-4625 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L 基本値 5.3

■該当製品の確認方法

影響を受ける製品とバージョンは以下の通りです。

シリーズ	製品形名		バージョン
MELSEC iQ-F シリーズ	FX5U-xMy/z x=32,64,80, y=T,R, z=ES,DS,ESS,DSS	製造番号 17X****以降	全バージョン
		製造番号 179****以前	1.060 以降
	FX5UC-xMy/z x=32,64,96, y=T, z=D,DSS	製造番号 17X****以降	全バージョン
		製造番号 179****以前	1.060 以降
	FX5UC-32MT/DS-TS, FX5UC-32MT/DSS-TS, FX5UC-32MR/DS-TS		全バージョン
	FX5UJ-xMy/z x=24,40,60, y=T,R, z=ES,DS,ESS,DSS		全バージョン
	FX5S-xMy/z x=30,40,60, y=T,R, z=ES,ESS		全バージョン
MELSEC iQ-R シリーズ	R00/01/02CPU		05 以降
	R04/08/16/32/120(EN)CPU		35 以降
	R08/16/32/120PCPU		37 以降

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-F FX5S/FX5UJ/FX5U/FX5UC ユーザーズマニュアル(ハードウェア編)
15.3 エンジニアリングツールによる確認 「ユニット診断」
・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」

各種製品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-F/iQ-R シリーズの CPU ユニットの Web サーバ機能には、過度な認証試行に対する不適切な制限(CWE-307[2])によるサービス拒否(DoS)の脆弱性が存在します。

■脆弱性がもたらす脅威

攻撃者が連続して不正に Web サーバ機能へのログインを試行することにより、攻撃者による不正なログイン試行後ある一定期間が経過するまで、正規ユーザによる Web サーバ機能へのログインができなくなる可能性があります。攻撃者による不正なログイン試行が続く限り、本脆弱性の影響が続きます。

■対策方法

軽減策・回避策にて対応をお願いいたします。

1 https://www.ipa.go.jp/security/vuln/CVSSv3.html
2 https://cwe.mitre.org/data/definitions/307.html

■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※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。

・当該製品および当該製品が接続された LAN への物理的なアクセスを制限してください。

※:IP フィルタ機能については、以下のマニュアルを参照ください。

MELSEC iQ-F FX5 ユーザーズマニュアル(Ethernet 通信編)「12.1 IP フィルタ機能」

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」

■謝辞

本脆弱性を報告いただいた、ELEX FEIGONG RESEARCH INSTITUTE of Elex CyberSecurity, Inc.の Peter Cheng 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

■改定履歴

2024 年 2 月 15 日

・該当製品に以下のシリーズを追加しました。

MELSEC iQ-R シリーズ

・上記に伴い、「概要」、「該当製品の確認方法」、「脆弱性の説明」及び「軽減策・回避策」を修正しました。