

MELSEC iQ-F CPU ユニットにおける情報漏えい、情報改ざんおよびサービス拒否(DoS)の脆弱性

公開日 2025 年 8 月 28 日
三菱電機株式会社

■概要

MELSEC iQ-F シリーズにおいて、重要な機能に対する認証の欠如(CWE-306¹)による情報漏えい、情報改ざんおよびサービス拒否(DoS)の脆弱性が存在することが判明しました。当該製品の MODBUS/TCP には認証の機能がないため、攻撃者は、当該製品のデバイス値の参照、変更を行える可能性があります。また、攻撃者は、プログラムの演算を停止させることができます。 (CVE-2025-7405)

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-2025-7405 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L 基本値:7.3

■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-xMT/y, FX5U-xMR/z x=32,64,80, y=ES,DS,ESS,DSS, z=ES,DS	1.060 以降
	FX5UC-xMy/z x=32,64,96, y=T, z=D,DSS	1.060 以降
	FX5UC-32MT/DS-TS, FX5UC-32MT/DSS-TS, FX5UC-32MR/DS-TS	1.060 以降
	FX5UJ-xMT/y, FX5UJ-xMR/z x=24,40,60, y=ES,DS,ESS,DSS, z=ES,DS	全バージョン
	FX5UJ-xMy/ES-A ^{※1} x=24,40,60, y=T,R	全バージョン
	FX5S-xMT/y, FX5S-xMR/z x=30,40,60,80 ^{※1} , y=ES,DS,ESS,DSS, z=ES,DS	全バージョン

※1:これらの製品は限定的な地域で販売されています。

■脆弱性の説明

MELSEC iQ-F シリーズにおいて、重要な機能に対する認証の欠如(CWE-306)による情報漏えい、情報改ざんおよびサービス拒否(DoS)の脆弱性が存在します。

■脆弱性がもたらす脅威

攻撃者は、当該製品のデバイス値の参照、変更を行える可能性があります。また、攻撃者は、プログラムの演算を停止させることができます。

■お客様での対応

対策版のリリース予定はございませんので、軽減策・回避策にて対応をお願いいたします。

■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^{※2}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。
- ・当該製品及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。

※2: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(通信編)「13.1 IP フィルタ機能」

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>

■謝辞

本脆弱性をご報告いただいた OPSWAT Unit515 の Thai Do 様、Minh Pham 様、及び Quan Le 様、Loc Nguyen 様に感謝いたします。

¹ <https://cwe.mitre.org/data/definitions/306.html>

² <https://www.ipa.go.jp/security/vuln/CVSSv3.html>

- 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>