

MELSEC iQ-F CPU ユニットにおける情報の漏えい 及びサービス拒否(DoS)の脆弱性

公開日 2025 年 5 月 29 日
三菱電機株式会社

■概要

MELSEC iQ-F CPU ユニットにおいて、情報の漏えい及びサービス拒否(DoS)の脆弱性が存在することが判明しました。攻撃者は、細工した不正なパケットを送信することにより、当該製品の情報を読み出す、若しくは MELSOFT 接続(GX Works3、GOT などの三菱電機 FA 製品との通信)をサービス停止(DoS)状態に、又は CPU ユニートを動作停止(DoS)状態に陥らせることができる可能性があります。(CVE-2025-3755)

■CVSS スコア¹

CVE-2025-3755 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H 基本値 9.1

■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	全バージョン
	FX5UC-xMy/z x=32,64,96, y=T, z=D,DSS	全バージョン
	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
	FX5UJ-xMy/ES-A ^{※1} x=24,40,60, y=T,R,	全バージョン
	FX5S-xMy/z x=30,40,60,80 ^{※1} , y=T,R, z= ES,DS,ESS,DSS	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 CPU ユニットには、入力で指定されたインデックス、位置、またはオフセットの不適切な検証(CWE-1285²)による情報の漏えい及びサービス拒否(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、細工した不正なパケットを送信することにより、当該製品の情報を読み出す、若しくは MELSOFT 接続をサービス停止(DoS)状態に、又は CPU ユニートを動作停止(DoS)状態に陥らせることができる可能性があります。なお、復旧には当該製品のリセットが必要になります。

■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>

■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>

¹ <https://www.ipa.go.jp/security/vuln/CVSSv3.html>

² <https://cwe.mitre.org/data/definitions/1285.html>