MELSEC iQ-F シリーズの FX5-ENET/IP 形 Ethernet ユニットにおけるサービス拒否(DoS)の脆弱性

公開日 2026 年 6 月 18 日
三菱電機株式会社

■概要

MELSEC iQ-F シリーズの FX5-ENET/IP 形 Ethernet ユニットにおいて、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。攻撃者は、当該製品の Ethernet ポートに対して短時間に大量の通信パケットを継続的に送信することにより、製品の処理負荷を増大させ、異常検知のための内部処理が行われないようにし、通信機能を停止させることで、当該製品をサービス停止(DoS)状態に陥らせることができる可能性があります(CVE-2026-8806)。

■CVSS スコア [1]

CVE-2026-8806　CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N 基本値:8.7

■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とおりです。

シリーズ	製品形名	バージョン
MELSEC iQ-F シリーズ	FX5-ENET/IP 形 Ethernet ユニット FX5-ENET/IP	全バージョン

■脆弱性の説明

MELSEC iQ-F シリーズの FX5-ENET/IP 形 Ethernet ユニットにおいて、予期せぬ動作(CWE-440[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

攻撃者は、当該製品の Ethernet ポートに対して短時間に大量の通信パケットを継続的に送信することにより、製品の処理負荷を増大させ、異常検知のための内部処理が行われないようにし、通信機能を停止させることで、当該製品をサービス停止(DoS)状態に陥らせることができる可能性があります

■お客様での対応

対策バージョンのリリース予定はございません。「■軽減策・回避策」に記載の軽減策・回避策にてご対応ください。
併せて、後継機種である FX5-EIP 形 EtherNet/IP ユニット FX5-EIP への移行をご検討ください。

■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、仮想プライベートネットワーク(VPN)等を使用し、不正な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。
・当該製品の 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。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」
　マニュアルは以下の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
・当該製品並びに当該製品へ接続可能なパソコン及びネットワーク機器への物理的なアクセスを制限してください。
・当該製品へアクセス可能なパソコンにウィルス対策ソフトを搭載してください。

■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.first.org/cvss/v4-0/specification-document

2 https://cwe.mitre.org/data/definitions/440.html