

MELSEC iQ-F シリーズの EtherNet/IP ユニット及び Ethernet ユニットの Ethernet 機能における複数のサービス拒否(DoS)の脆弱性

公開日 2026 年 3 月 3 日
三菱電機株式会社

■概要

MELSEC iQ-F シリーズの EtherNet/IP ユニット及び Ethernet ユニットの Ethernet 機能において、複数のサービス拒否(DoS)の脆弱性が存在することが判明しました。攻撃者は、該当製品に対して継続的に UDP パケットを送信し続けることにより、該当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-2026-1874、CVE-2026-1875、CVE-2026-1876)。

■CVSS スコア¹

CVE-2026-1874 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
CVE-2026-1875 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
CVE-2026-1876 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。

CVE-2026-1874

- ・ MELSEC iQ-F FX5-ENET/IP 形 Ethernet ユニット FX5-ENET/IP Ver.1.106 以前
- ・ MELSEC iQ-F FX5-EIP 形 EtherNet/IP ユニット FX5-EIP 全バージョン

CVE-2026-1875

- ・ MELSEC iQ-F FX5-EIP 形 EtherNet/IP ユニット FX5-EIP 全バージョン

CVE-2026-1876

- ・ MELSEC iQ-F FX5-ENET/IP 形 Ethernet ユニット FX5-ENET/IP 全バージョン

【バージョン確認方法】

MELSEC iQ-F FX5-ENET/IP 形 Ethernet ユニット FX5-ENET/IP

ファームウェアバージョンの確認方法は、MELSEC iQ-F FX5-ENET/IP 形 Ethernet ユニットユーザーズマニュアル「付 4 バッファメモリ」「バッファメモリ詳細」「ファームウェアバージョン」を参照ください。

MELSEC iQ-F FX5-EIP 形 EtherNet/IP ユニット FX5-EIP

ファームウェアバージョンの確認方法は、MELSEC iQ-F FX5-EIP 形 EtherNet/IP ユニットユーザーズマニュアル「付 4 バッファメモリ」「バッファメモリ詳細(ユニット状態 G29~G207)」「共通エリア(ユニット情報)」を参照ください。

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>

■脆弱性の説明

MELSEC iQ-F シリーズの EtherNet/IP ユニット及び Ethernet ユニットの Ethernet 機能において、以下の 3 件のサービス拒否の脆弱性が存在します。

CVE ID	脆弱性の説明
CVE-2026-1874	常に不適切な制御フローの実装(CWE-670 ²)によるサービス拒否の脆弱性
CVE-2026-1875	リソースの不適切なシャットダウンおよびリリース(CWE-404 ³)によるサービス拒否(DoS)の脆弱性
CVE-2026-1876	リソースの不適切なシャットダウンおよびリリース(CWE-404)によるサービス拒否(DoS)の脆弱性

■脆弱性がもたらす脅威

攻撃者は、当該製品に対して継続的に UDP パケットを送信し続けることにより、受信バッファの枯渇を発生させ、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。復旧には当該製品の再起動が必要になります。

¹ <https://www.first.org/cvss/v4-0/specification-document>

² <https://cwe.mitre.org/data/definitions/670.html>

³ <https://cwe.mitre.org/data/definitions/404.html>

■お客様での対応

CVE-2026-1874

FX5-ENET/IP をご使用のお客様は、以下のサイトから、「■製品での対応」に記載の対策済みバージョンのアップデートファイルをダウンロードしたうえで、アップデートしてください。アップデートの方法は、MELSEC iQ-F FX5 ユーザーズマニュアル(応用編)「9.2 エンジニアリングツールを使用するアップデート方法」「インテリジェント機能ユニットのファームウェアアップデート」を参照ください。

FX5-EIP に対しては、近日中に対策バージョンをリリース予定です。それまでの間は、「■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。

CVE-2026-1875

近日中に対策バージョンをリリース予定です。それまでの間は、「■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。

CVE-2026-1876

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。

サイト:

<https://www.mitsubishielectric.co.jp/fa/download/index.html>

■製品での対応

対策済の製品及びバージョンは以下のとおりです。

CVE-2026-1874

MELSEC iQ-F FX5-ENET/IP 形 Ethernet ユニット FX5-ENET/IP Ver.1.107 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、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」

- ・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イ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>