



公開日: 2024/11/19 最終更新日: 2026/03/31

JVNVU#97790713

三菱電機製MELSEC iQ-Fにおける指定されたタイプの入力に対する不適切な検証の脆弱性

概要

三菱電機製MELSEC iQ-F EthernetユニットおよびEtherNet/IPユニットには、指定されたタイプの入力に対する不適切な検証の脆弱性が存在します。

影響を受けるシステム

- MELSEC iQ-F シリーズ
 - FX5-ENET 1.100~1.200
 - FX5-ENET/IP 1.100~1.104

バージョンの確認方法等詳細については、開発者が提供する情報を確認してください。

詳細情報

三菱電機株式会社が提供するMELSEC iQ-F EthernetユニットおよびEtherNet/IPユニットのEthernetポートには、指定されたタイプの入力に対する不適切な検証 (CWE-1287、CVE-2024-8403) の脆弱性が存在します。

想定される影響

遠隔の第三者によって細工された不正なSLMPパケットを受信すると、当該ユニットのEthernet通信が、サービス運用妨害 (DoS) 状態になる可能性があります。

対策方法

アップデートする

[ダウンロード](#) | [三菱電機FA](#)から、対策済みバージョンのファームウェアアップデート情報ファイルをダウンロードし、アップデートしてください。

アップデートの方法等詳細については、開発者が提供する情報を確認してください。

ワークアラウンドを実施する

次の回避策を適用することで、本脆弱性の影響を軽減することが可能です。

- 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する
- 当該製品、当該製品と同一のネットワーク内に配置されたパソコンおよびネットワーク機器への物理的なアクセスを制限する
- 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する
- 当該製品のIPフィルタ機能 (*1) 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する

(*1) IPフィルタ機能については、以下のマニュアルを参照してください。

- 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」

ベンダ情報

ベンダ	リンク
三菱電機株式会社	MELSEC iQ-F EthernetユニットおよびEtherNet/IPユニットのEthernetポートにおけるサービス拒否(DoS)の脆弱性

参考情報

- [ICS Advisory | ICSA-24-324-01](#)
Mitsubishi Electric MELSEC iQ-F Series

JVN

[HOME](#)[JVNとは](#)[脆弱性レポートの読み方](#)[脆弱性レポート一覧](#)[VN-JP](#)[VN-JP \(調整不能\)](#)[VN-VU](#)[TA](#)[TRnotes](#)[JVN iPedia](#)[脆弱性対策情報データベース](#)[MyJVN](#)[JVNJS/RSS](#)[ベンダ情報一覧](#)[連絡不能開発者一覧](#)[脆弱性情報の届出](#)[お問合せ先](#)

JPCERT/CCからの補足情報

JPCERT/CCによる脆弱性分析結果

CVSS v3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

基本値: 7.5 ▼

謝辞

この脆弱性情報は、製品利用者への周知を目的に、開発者がJPCERT/CCに報告し、JPCERT/CCが開発者との調整を行いました。

関連文書

[JPCERT 緊急報告](#)[JPCERT REPORT](#)[CERT Advisory](#)[CPNI Advisory](#)[TRnotes](#)[CVE](#)[JVN iPedia](#)

更新履歴

2024/11/20

[参考情報] にICS Advisoryのリンクを追加しました

2026/03/31

[影響を受けるシステム]、[対策方法] を更新しました

Copyright (c) 2000-2026 JPCERT/CC and IPA. All rights reserved.