



公開日：2025/05/14 最終更新日：2026/02/03

## JVNVU#96620683 三菱電機製FA製品のEthernet機能におけるサービス運用妨害 (DoS) の脆弱性

### 概要

三菱電機製FA製品のEthernet機能には、サービス運用妨害 (DoS) の脆弱性が存在します。

### 影響を受けるシステム

- CC-Link IE TSNリモートI/Oユニット
- CC-Link IE TSNアナログ-デジタル変換ユニット
- CC-Link IE TSNデジタル-アナログ変換ユニット
- CC-Link IE TSN FPGAユニット
- CC-Link IE TSN リモート局用GbE-PHY内蔵通信LSI CP620
- MELSEC iQ-Rシリーズ CC-Link IE TSN マスタ・ローカルユニット
- MELSEC iQ-RシリーズEthernet インタフェースユニット
- CC-Link IE TSN マスタ局・ローカル局用通信LSI CP610
- MELSEC iQ-Fシリーズ CC-Link IE TSN マスタ・ローカルユニット
- MELSEC iQ-Fシリーズ Ethernetユニット
- MELSEC iQ-Fシリーズ FX5-ENET/IP形Ethernetユニット

上記影響を受ける「製品名/シリーズ名」の「形名」および「バージョン」、バージョン確認方法の詳細については、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複数のFA製品のEthernet機能には、入力で指定された数量の不適切な検証に起因するサービス運用妨害 (DoS) の脆弱性 (CWE-1284、CVE-2025-3511) が存在します。

### 想定される影響

攻撃者によって細工された不正なUDPパケットを受信することで、次のような影響を受ける可能性があります。

- 当該製品がサービス運用妨害 (DoS) 状態となる
- CC-Link IEF Basicの通信においてタイムアウトエラーが発生する
- シンプルCPU通信において通信遅延が発生する

詳しくは、開発者が提供する情報を確認してください。

### 対策方法

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

脆弱性対象情報データベース

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

### アップデートする

対策バージョンが提供されている製品については、開発者が提供する情報をもとに、ファームウェアまたはCP620用サンプルコードを対策済バージョンにアップデートしてください。

対策済バージョンやアップデート手順等の詳細については、開発者が提供する情報を参照してください。

### ワークアラウンドを実施する

対策バージョンが提供されていない製品については、対策バージョンが提供されるまでの間、開発者は次の回避策・軽減策の適用を推奨しています。

- 該当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) 等で不正アクセスを防止する
- 該当製品をLAN内で使用し、信頼できないネットワークやホスト、ユーザからのアクセスをブロックする
- 該当製品および当該製品に接続可能なPCへの物理的なアクセスを制限する

詳しくは、開発者が提供する情報を確認してください。

---

## ベンダ情報

ベンダ	リンク
三菱電機株式会社	<a href="#">複数のFA製品のEthernet機能におけるサービス拒否 (DoS) の脆弱性</a>

---

## 参考情報

1. [ICS Advisory | ICSA-25-128-03](#)  
Mitsubishi Electric CC-Link IE TSN

---

## JPCERT/CCからの補足情報

---

## JPCERT/CCによる脆弱性分析結果

### 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](#)

## 更新履歴

**2025/10/09**

[影響を受けるシステム]、[詳細情報]、[想定される影響]、[対策方法] を更新しました

**2026/02/03**

[影響を受けるシステム]、[想定される影響]、[対策方法] を更新しました

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