CC-Link IE TSN 対応製品における
情報改ざん及びサービス拒否(DoS)の脆弱性

公開日 2026 年 11 月 9 日
三菱電機エンジニアリング株式会社

■概要

CC-Link IE TSN 通信プロトコルにおいて、情報改ざん及びサービス拒否(DoS)の脆弱性が存在することが判明しました。CC-Link IE TSN ネットワークへアクセス可能な攻撃者は、不正なパケットを特定のタイミングで送信することにより、通信データを改ざんできる可能性があります(CVE-2026-13584)。これにより、攻撃者が、機器の制御を妨害したり誤動作を引き起こしたりすることで、対象機器をサービス停止(DoS)状態に陥らせることができる可能性があります。

■CVSS スコア[1]

CVE-2026-13584 CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:N/VI:H/VA:L/SC:N/SI:N/SA:N 基本値 7.1

■該当製品の確認方法

該当製品は以下のとおりです。

No.	製品名	形名	バージョン
1	デジタル信号変換器(ターミナルユニット)用 CC-Link IE TSN/Ethernet 対応ネットワークインタフェースユニット	FA3-TH1T16XC FA3-TH1T16XC-01C FA3-TH1T16Y FA3-TH1T16Y-01C FA3-TH1T16YE FA3-TH1T16YE-01C FA3-TH1M16XC FA3-TH1M16XC-01C FA3-TH1M16Y FA3-TH1M16Y-01C FA3-TH1M16YE FA3-TH1M16YE-01C	全バージョン
2	アナログ信号変換器用 CC-Link IE TSN/Ethernet 対応ネットワークインタフェースユニット	FA3-AT1T8X FA3-AT1T8X-01C FA3-AT1T8Y FA3-AT1T8Y-01C FA3-AT1M8X FA3-AT1M8X-01C FA3-AT1M8Y FA3-AT1M8Y-01C	全バージョン
3	CC-Link IE TSN－CC-Link ブリッジユニット	FA3-BR1TC	全バージョン

■脆弱性の説明

CC-Link IE TSN 通信プロトコルにおいて、通信チャネルで送信中のメッセージの整合性への不適切な強制(CWE-924[2])による、通信データの改ざん及びサービス拒否(DoS)の脆弱性が存在します。

---

[1] https://www.first.org/cvss/v4-0/specification-document

[2] https://cwe.mitre.org/data/definitions/924.html

■脆弱性がもたらす脅威

CC-Link IE TSN へアクセス可能な攻撃者は、不正なパケットを特定のタイミングで送信することで、通信データ(制御の入出力値)を改ざんすることができる可能性があります。これにより、攻撃者が、機器の制御を妨害したり誤動作を引き起こしたりすることで、対象機器をサービス停止(DoS)状態に陥らせることができる可能性があります。

■対策方法

「■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。

■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、三菱電機エンジニアリングは以下に示す軽減策を講じることを推奨します。

・攻撃者が攻撃端末を接続することを防ぐため、当該製品及び当該製品が接続された CC-Link IE TSN ネットワークへの物理的なアクセスを、以下のような方法で制限してください。
  a) 設置場所の入退出管理
  b) 当該製品及びネットワーク機器を設置した制御盤の施錠
  c) Ethernet ポートのロック（ロックアクセサリの利用など）
・該当製品を、信頼できないネットワークやホストとの通信をファイアウォールなどでブロックされた信頼済みのネットワーク内で使用してください。
・信頼済みのネットワークと外部ネットワークの境界に設置する機器に対して、認証情報及びアクセス権限を適切に設定してください。

■お客様からのお問い合わせ先

以下 Web ページ内の「FA グッズ」からお問い合わせください。
〈製品・技術・サービスに関するお問い合わせ | FA 関連製品〉
https://www.mee.co.jp/contact2/list.html