

CC-Link IE TSN 通信プロトコルにおける 情報改ざん及びサービス拒否(DoS)の脆弱性

公開日 2026 年 7 月 30 日
三菱電機株式会社

■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すことで、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

該当製品は以下の通りです。

No.	製品名	形名	バージョン
1	MELSEC MX コントローラ MX-R モデル	MXR300-16/32/64 MXR500-128/256	全バージョン
2	MELSEC MX コントローラ MX-F モデル	MXF100-8-N32/P32 MXF100-16-N32/P32	全バージョン
3	マスタ・ローカルユニット	RJ71GN11-T2/SX/EIP	全バージョン
4		FX5-CCLGN-MS	全バージョン
5	CC-Link IE TSN インタフェースボード	NZ81GN11-SX/T2	全バージョン
6	モーションユニット	RD78G4/G8/G16/G64 RD78GHV/GHW	全バージョン
7		FX5-40SSC-G FX5-80SSC-G	全バージョン
8		MR-EM441G	全バージョン
9	ブロックタイブリモートユニット	NZ2GN2S1-32D/32T/32TE/32DT/32DTE NZ2GN2B1-32D/32T/32TE/32DT/32DTE NZ2GNCF1-32D/32T NZ2GNCE3-32D/32DT NZ2GN12A4-16D/16DE NZ2GN12A2-16T/16TE NZ2GN12A42-16DT/16DTE NZ2GN2S1-16D/16T/16TE NZ2GN2B1-16D/16T/16TE	全バージョン
10	安全機能付きブロックタイブリモートユニット	NZ2GNSS2-8D/8TE/16DTE (-K モデル含む) NZ2GNS12A2-14DT/16DTE	全バージョン
11	アナログーデジタル変換ユニット	NZ2GN2S-60AD4 NZ2GN2B-60AD4	全バージョン
12	デジタルーアナログ変換ユニット	NZ2GN2S-60DA4 NZ2GN2B-60DA4	全バージョン
13	CC-Link IE TSN 対応カプラユニット ^{※1}	NZ2FT-GN	全バージョン
14	FPGA ユニット	NZ2GN2S-D41P01/D41D01/D41PD02	全バージョン
15	テンションメータ	LM7-1LG LM7-2LG	全バージョン
16	AC サーボ MELSERVO-J5 シリーズ	MR-J5-G MR-J5W-G MR-J5-G-HS/RJ/LL MR-J5D-G4 MR-MD333G	全バージョン

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

17	AC サーボ MELSERVO-JET シリーズ※ ¹	MR-JET-G/G4-HS	全バージョン
18	リニアトラックシステム MTR-S シリーズ リニアトラック制御ユニット※ ¹	MTR-SCU00-4G/PG	全バージョン
19	インバータ FR-A800/F800/E800 シリーズ	FR-A8NCG FR-A8NCG-S FR-A800-GN FR-E800-E/SCE	全バージョン
20	産業用ロボット CR800-D シリーズコントローラ ネットワークベースカード	2F-DQ535-TSN	全バージョン
21	数値制御装置 M800V/M80V シリーズ用 CC-Link IE TSN 拡張ユニット	FCU8-EX569	全バージョン
22	CC-Link IE TSN-CC-Link IE フィールド ネットワークブリッジユニット	NZ2GN-GFB	全バージョン
23	CC-Link IE TSN-AnyWireASLINK ブリッジユニット	NZ2AW1GNAL	全バージョン
24	エネルギー計測ユニット CC-Link IE TSN 通信ユニット	EMU4-CM-TSN	全バージョン
25	産業用 PC MELIPC シリーズ	MI2532-W MI2332-W	全バージョン
26	GOT3000 シリーズ	GT3715-FHCB GT3712-WXCB GT3715-XRBA/XRBD GT3712-XRBA/XRBD GT3710-XRBA/XRBD GT3708-XRBA/XRBD	全バージョン
27	CC-Link IE TSN 通信ユニット	GT25-J71GN13-T2	全バージョン
28	モーションソフトウェア	SWM-G SWM-G-N1	全バージョン
29	CC-Link IE TSN 通信ソフトウェア Windows 版	SW1DND-CCICTCT-M	全バージョン
30	分析支援ソフトウェア MELSOFT VIMA※ ¹	SW1DNN-VIMA-M	全バージョン
31	マスタ局・ローカル局用通信 LSI(デバイスキット)	NZ2KT-NPETNG51	全バージョン
32	CC-Link IE TSN マスタ局・ローカル局用通信 LSI (専用通信 LSI)	NZ2GACP610-60	全バージョン
33	リモート局用 GbE-PHY 内蔵通信 LSI	NZ2GACP620-60/300 NZ2GACP621-90/720	全バージョン
34	CC-Link IE TSN マスタ局・ローカル局用通信 LSI (ソースコード開発キット)	SW1DNN-GN610SRC-M	全バージョン
35	リモート局用ソフトウェア開発キット	SW1DNC-GNSDK1S-M SW1DNC-GNSDK2S-M	全バージョン

※1:これらの製品は限定的な地域で販売されています。

■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-924²)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。

■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すことで、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。

■お客様での対応

「■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)

² <https://cwe.mitre.org/data/definitions/924.html>

- ・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。

■謝辞

この脆弱性をご報告いただいた Nozomi Networks, Inc.の Alessandro Di Pinto 様、Giovanni Dini Gentilini 様、Luca Cremona 様、ならびに Gabriele Quagliarella 様に感謝いたします。

■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>