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

公開日 2025 年 4 月 25 日
最終公開日 2025 年 10 月 9 日
三菱電機株式会社

■概要

複数の FA 製品の Ethernet 機能において、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、当該製品に対して不正な UDP パケットを送信することにより、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。(CVE-2025-3511)

■CVSS スコア [1]

CVE-2025-3511　CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H 基本値 7.5

■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通りです。

No.	製品名/シリーズ名	形名	バージョン
1	CC-Link IE TSN リモート I/O 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	09 以前
2	CC-Link IE TSN アナログ－デジタル変換ユニット	NZ2GN2S-60AD4 NZ2GN2B-60AD4	07 以前
3	CC-Link IE TSN デジタル－アナログ変換ユニット	NZ2GN2S-60DA4 NZ2GN2B-60DA4	07 以前
4	CC-Link IE TSN FPGA ユニット	NZ2GN2S-D41P01/D41D01/D41PD02	01
5	CC-Link IE TSN リモート局用 GbE-PHY 内蔵通信 LSI CP620	NZ2GACP620-300/60	1.08J 以前
6	MELSEC iQ-R シリーズ CC-Link IE TSN マスタ・ローカルユニット	RJ71GN11-T2	26 以前
7		RJ71GN11-EIP	10 以前
8		RJ71GN11-SX	05 以前
9	MELSEC iQ-R シリーズ Ethernet インタフェースユニット	RJ71EN71	85 以前
10	CC-Link IE TSN マスタ局・ローカル局用通信 LSI CP610	NZ2GACP610-60 NZ2KT-NPETNG51	05 以前

【バージョン確認方法】

No.1-4,10:「CC-Link IE TSN ファームウェアアップデートツール」にて、ファームウェアバージョンを確認してください。
詳細な手順は、「CC-Link IE TSN ファームウェアアップデートツール」のヘルプを参照ください。

No.5 :CP620 用サンプルコードのインストールを行い、作成されたフォルダ内の「version.txt」にて、CP620 サンプルコードのバージョンを確認してください。CP620 用サンプルコードの入手方法及びインストール方法は、「■お客様での対応」の【更新手順】を参照ください。

No.6-9:ファームウェアバージョンの確認方法は、MELSEC iQ-R ユニット構成マニュアル「付 1 製造情報・ファームウェアバージョン」を参照ください。マニュアルは以下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

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(CWE-1284[2])に起因するサービス拒否(DoS)の脆弱性が存在します。

■脆弱性がもたらす脅威

攻撃者は、該当製品に対して不正な UDP パケットを送信することにより、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。

1 https://www.ipa.go.jp/security/vuln/scap/cvssv3.html
2 https://cwe.mitre.org/data/definitions/1284.html

No.1～5 の該当製品が、攻撃者からの不正な UDP パケットを受信した後に、3 秒以内に正常な UDP パケットを受信しない場合に、脅威が発現します。復旧には当該製品の再起動が必要になります。
No.6～10 の該当製品が、不正な UDP パケットを受信することにより、サービス停止（DoS）状態に陥ることがあります。復旧には当該製品の再起動が必要になります。

■お客様での対応
該当製品をご使用のお客様は、以下に示す手順に従って、ファームウェア又は CP620 用サンプルコードを「■製品での対応」に記載の対策済みのバージョンに更新してください。

【更新手順】
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又は CP620 用サンプルコード、ファームウェアバージョンアップ用エンジニアリングソフトウェア及びマニュア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。
https://www.mitsubishielectric.co.jp/fa/download/index.html
アップデートの方法は、以下を参照ください。
No.1-4,10：
・CC-Link IE TSN ファームウェアアップデートツール リファレンスマニュアル「2. ファームウェアアップデートの手順」
No.5：
・CP620 用サンプルコードは、ダウンロードしたファイル内の「SW1DNC-GN620SRC-M.exe」を実行することでインストール可能です。
No.6-9：
・MELSEC iQ-R ユニット構成マニュアル 「付 2 ファームウェアアップデート機能」

■製品での対応
対策済の製品およびバージョンは、以下となります。

No.	製品名/シリーズ名	形名	該当ファームウェアの対策バージョン
1	CC-Link IE TSN リモート I/O 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	10 以降
2	CC-Link IE TSN アナログ-デジタル変換ユニット	NZ2GN2S-60AD4 NZ2GN2B-60AD4	08 以降
3	CC-Link IE TSN デジタル-アナログ変換ユニット	NZ2GN2S-60DA4 NZ2GN2B-60DA4	08 以降
4	CC-Link IE TSN FPGA ユニット	NZ2GN2S-D41P01/D41D01/D41PD02	02 以降
5	CC-Link IE TSN リモート局用 GbE-PHY 内蔵通信 LSI CP620	NZ2GACP620-300/60	1.09K 以降
6	MELSEC iQ-R シリーズ CC-Link IE TSN マスタ・ローカルユニット	RJ71GN11-T2	28 以降
7		RJ71GN11-EIP	13 以降
8		RJ71GN11-SX	07 以降
9	MELSEC iQ-R シリーズ Ethernet インタフェースユニット	RJ71EN71	86 以降
10	CC-Link IE TSN マスタ局・ローカル局用通信 LSI CP610	NZ2GACP610-60 NZ2KT-NPETNG51	06 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ィ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

■更新履歴

2025 年 10 月 9 日

該当製品の確認方法、脆弱性がもたらす脅威、お客様での対応、製品での対応を改訂しました。

影響を受ける製品に RJ71GN11-T2、RJ71GN11-EIP、RJ71GN11-SX、RJ71EN71、NZ2GACP610-60、NZ2KT-NPETNG51 を追加しました。