MELSEC シリーズ リモート I/O の TCP/IP プロトコルスタックにおける複数のサービス拒否(DoS)の脆弱性

公開日 2021 年 12 月 16 日
最終更新日 2024 年 4 月 18 日
三菱電機株式会社

■概要

MELSEC シリーズ リモート I/O の TCP/IP プロトコルスタックには、不適切な入力値検証(CWE-20)による複数のサービス拒否(DoS)の脆弱性が存在することが判明しました。当該製品には、攻撃者が細工したパケットを送信することによって、サービス停止(DoS)状態に陥る可能性があります。(CVE-2020-35683、CVE-2020-35684、CVE-2021-31401)

■CVSS スコア [1]

CVE-2020-35683 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H 基本値:7.5
CVE-2020-35684 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H 基本値:7.5
CVE-2021-31401 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

次の製品形名とバージョンのものが影響を受けます。

MELSEC シリーズ リモート I/O※

形名	バージョン
NZ2FT-EIP	全てのバージョン
NZ2FT-MT	
NZ2FT-PN	
NZ2FT-GN	
NZ2FT-PBV	
NZ2FT-BT	

※地域限定的に販売している製品です。

■脆弱性の説明

MELSEC シリーズ リモート I/O の TCP/IP プロトコルスタックには、不適切な入力値検証(CWE-20[2])による複数のサービス拒否(DoS)の脆弱性(CVE-2020-35683、CVE-2020-35684、CVE-2021-31401)が存在します。

■脆弱性がもたらす脅威

当該製品には、攻撃者が細工したパケットを送信することによって、サービス停止(DoS)状態に陥る可能性があります。

■お客様での対応

対策版のリリース予定はございませんので、該当製品をご使用のお客様は、軽減策・回避策にて対応をお願いいたします。

■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減に抑えるため、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、ルータ、ファイアウォール等の設置や仮想プライベートネットワーク(VPN)の利用などにより、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。
・当該製品及び当該製品が接続されたネットワーク上の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。(例:鍵付きキャビネットへの格納、不使用 Ethernet/USB ポートへのシール貼付)

■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

2024 年 4 月 18 日
対策方法の記載を変更。

1 https://www.ipa.go.jp/security/vuln/CVSSv3.html
2 https://cwe.mitre.org/data/definitions/20.html