MELSEC Q および L シリーズ CPU ユニットの Ethernet ポートにおけるサービス拒否(DoS)の脆弱性

公開日 2022 年 6 月 14 日
三菱電機株式会社

■概要

MELSEC Q および L シリーズの CPU ユニットには、不適切なリソースロック(リソースの解放の不備)によるサービス拒否(DoS)の脆弱性が存在することが判明しました。攻撃者から不正なパケットを受信すると、当該 CPU ユニットの Ethernet 通信がサービス停止(DoS)状態)に陥る可能性があります。(CVE-2022-24946)

この脆弱性の影響を受ける製品形名およびバージョンを以下に示します。

■CVSS スコア

CVE-2022-24946 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

影響を受ける製品の形名、シリアル No.は以下の通りです。

シリーズ	形名	バージョン
Q シリーズ	Q03UDECPU、Q04/06/10/13/20/26/50/100UDEHCPU	全バージョン
	Q03/04/06/13/26UDVCPU	シリアル No.の上 5 桁"24051"以前
	Q04/06/13/26UDPVCPU	シリアル No.の上 5 桁"24051"以前
L シリーズ	L02/06/26CPU(-P)、L26CPU-(P)BT	シリアル No.の上 5 桁"24051"以前

シリアル No.の確認方法は、以下のマニュアルを参照ください。

・「QCPU ユーザーズマニュアル(ハードウェア設計・保守点検編)」の「付 5 シリアル No.と機能バージョンの確認方法」

・「MELSEC-L CPU ユニットユーザーズマニュアル(ハードウェア設計・保守点検編)」の「付 5 シリアル No.と機能バージョンの確認方法」

■脆弱性の説明

MELSEC Q および L シリーズの CPU ユニットには、不適切なリソースロック(CWE-413)による DoS の脆弱性が存在します。

■脆弱性がもたらす脅威

攻撃者から不正なパケットを受信すると、Ethernet 通信が DoS 状態に陥ります。なお、復旧にはリセットが必要になります。

■対策方法

下記ユニットにおいて、不正なパケットを受信しても、Ethernet 通信が停止しないよう対策済です。

シリーズ	形名	バージョン
Q シリーズ	Q03/04/06/13/26UDVCPU	シリアル No.の上 5 桁"24052"以降
	Q04/06/13/26UDPVCPU	シリアル No.の上 5 桁"24052"以降
L シリーズ	L02/06/26CPU(-P)、L26CPU-(P)BT	シリアル No.の上 5 桁"24052"以降

上記以外のユニットについては、近日対応予定です。

■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。

■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