MELSEC Q シリーズ C 言語コントローラユニットの DHCP クライアント機能におけるサービス拒否(DoS)及び 悪意のあるプログラムが実行される脆弱性

公開日 2022 年 4 月 7 日
三菱電機株式会社

■概要

Wind River 社製のリアルタイム OS である VxWorks バージョン 6.4 の DHCP クライアント機能に、サービス拒否(DoS)及び悪意のあるプログラムが実行される脆弱性が存在することが報告されました。攻撃者は、該当製品に対して不正な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)状態に陥らせたり、悪意のあるプログラムを実行できる可能性があります。(CVE-2021-29998)

この脆弱性の影響を受ける MELSEC C 言語コントローラユニットの形名およびバージョンを以下に示します。

■CVSS スコア

CVE-2021-29998 CVSS:3.1 /AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H 基本値:9.0

■該当製品の確認方法

影響を受ける製品の形名、およびシリアル No.は以下の通りです。

形名	バージョン
Q12DCCPU-V	シリアル No.の上 5 桁"24031"以前

シリアル No.の確認方法は、以下を参照ください。

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

■脆弱性の説明

MELSEC Q シリーズ C 言語コントローラユニットには、VxWorks の DHCP クライアント機能におけるヒープベースのバッファオーバーフロー(CWE-122)による、サービス拒否(DoS)及び悪意のあるプログラムが実行される脆弱性が存在します。

■脆弱性がもたらす脅威

攻撃者には、不正な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)状態に陥らせたり、悪意のあるプログラムを実行できる可能性があります。なお、サービス停止(DoS)状態からの復旧には当該製品のリセットが必要です。

■対策方法

下記に記載のバージョンで対策済みです。

形名	バージョン
Q12DCCPU-V	シリアル No.の上 5 桁"24032"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。

・機能拡張モードを使用しており、かつ DHCP クライアント機能を使用していない場合は、C 言語コントローラ設定・モニタツールの"セキュリティ設定"で DHCP 機能を無効にしてください。
・お使いの DHCP サーバを最新版へアップデートしてください。
・当該製品を含むシステム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、システムへの不正アクセスを防止してください。
・当該製品をルータやファイアウォールで適切に区分された信頼できる LAN 内で使用してください。

■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