

MELSEC C 言語コントローラユニット及び MELIPC シリーズ MI5000 の TCP/IP 機能における複数の脆弱性

公開日 2020 年 2 月 14 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 6.5 以降の TCP/IP 機能 (IPnet) に、複数の脆弱性があることが報告されました。該当製品がネットワークに接続されている場合に、遠隔の攻撃者によって細工された TCP パケットを受信すると、当該製品のサービスが停止する、あるいは悪意のあるプログラムが実行される可能性があります。この問題の影響を受ける MELSEC C 言語コントローラユニット及び MELIPC シリーズ MI5000 のバージョンを以下に示しますので、該当製品については対策方法、あるいは軽減策に記載の内容を実施してください。

■該当製品の確認方法

影響を受ける製品及び対象の Ethernet ポートは以下のとおりです。

【MELSEC-Q シリーズ C 言語コントローラユニット】

・Q24DHCCPU-V、Q24DHCCPU-VG ユーザ Ethernet ポート(CH1、CH2)： シリアル No.の上 5 桁が”21121”以前
ユニットのシリアル No.は、定格銘板やユニット前面のシリアル No.表示板、MELSEC C 言語コントローラ設定・モニタツールのシステムモニタで確認できます。

【MELSEC iQ-R シリーズ C 言語コントローラユニット・C 言語インテリジェント機能ユニット】

・R12CCPU-V Ethernet ポート(CH1、CH2)： シリアル No.の上 2 桁が”11”以下
ユニットのシリアル No.は、定格銘板やユニット前面のシリアル No.表示板、CW Configurator のシステムモニタで確認できます。

・RD55UP06-V Ethernet ポート： シリアル No.の上 2 桁が”08”以下

ユニットのシリアル No.は、定格銘板やユニット前面のシリアル No.表示板、GX Works3 のシステムモニタで確認できます。

【MELIPC シリーズ MI5000】

・MI5122-VW Ethernet ポート(CH1)： シリアル No.の上 2 桁、もしくはファームウェアバージョンが”03”以下
ユニットのシリアル No.は、定格銘板やユニット前面のシリアル No.表示板、ファームウェアバージョンは MI Configurator の MELIPC 診断で確認できます。

■脆弱性の説明

MELSEC C 言語コントローラユニット及び MELIPC シリーズ MI5000 には、VxWorks の TCP/IP 機能 (IPnet) に起因する次の複数の脆弱性が存在します。

- ・Q24DHCCPU-V、Q24DHCCPU-VG
CVE-2019-12255/12257/12258/12259/12261/12262/12263/12264/12265
- ・R12CCPU-V、RD55UP06-V
CVE-2019-12256/12258/12259/12261/12262/12263/12264/12265
- ・MI5122-VW
CVE-2019-12256/12258/12259/12260/12261/12262/12263/12264/12265

■脆弱性がもたらす脅威

攻撃者により細工された TCP パケットを受信すると、製品のサービスが停止する、あるいは悪意のあるプログラムが実行される可能性があります。

■対策方法

製品のセキュリティ強化のため、以下のバージョンで TCP/IP 機能の脆弱性対策を実施しています。

【MELSEC-Q シリーズ C 言語コントローラユニット】

・Q24DHCCPU-V、Q24DHCCPU-VG： シリアル No.の上 5 桁が” 21122”以降

【MELSEC iQ-R シリーズ C 言語コントローラユニット・C 言語インテリジェント機能ユニット】

・R12CCPU-V： シリアル No.の上 2 桁が”12”以上

・RD55UP06-V： シリアル No.の上 2 桁が”09”以上

【MELIPC シリーズ MI5000】

・MI5122-VW： シリアル No.の上 2 桁が”04”以上、もしくはファームウェアバージョンが”04”以上

■軽減策

製品へのアクセスを、信頼できるネットワークからのアクセスに制限してください。

■お客様からのお問い合わせ先

製品をご購入いただいた弊社の支社、代理店にご相談ください。