MELSEC iQ-R シリーズの各種情報／ネットワークユニットの TCP/IP 機能における複数の脆弱性

公開日 2020 年 10 月 29 日
三菱電機株式会社

■概要

MELSEC iQ-R シリーズ EtherNet/IP ネットワークインタフェースユニット、PROFINET IO コントローラユニット、高速データロガーユニット、MES インタフェースユニットおよび OPC UA サーバユニットの TCP/IP スタックに複数の脆弱性が存在することが判明しました。この脆弱性を悪用された場合、悪意ある第三者の攻撃により、ネットワーク機能を停止、または悪意のあるプログラムを実行されてしまう危険性があります。(CVE-2020-5653、CVE-2020-5654、CVE-2020-5655、CVE-2020-5656、CVE-2020-5657、CVE-2020-5658)

この問題の影響を受ける MELSEC iQ-R シリーズ EtherNet/IP ネットワークインタフェースユニット、PROFINET IO コントローラユニット、高速データロガーユニット、MES インタフェースユニット、OPC UA サーバユニット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。

■CVSS スコア

CVE-2020-5653	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	基本値:9.8
CVE-2020-5654	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	基本値:7.5
CVE-2020-5655	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	基本値:7.5
CVE-2020-5656	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	基本値:9.8
CVE-2020-5657	CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H	基本値:7.1
CVE-2020-5658	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	基本値:5.3

■該当製品の確認方法

影響を受ける製品は以下の通りです。

【MELSEC iQ-R シリーズ EtherNet/IP ネットワークインタフェースユニット】
・RJ71EIP91： シリアル No の上 2 桁が"02"以下
【MELSEC iQ-R シリーズ PROFINET IO コントローラユニット】
・RJ71PN92： シリアル No の上 2 桁が"01"以下
【MELSEC iQ-R シリーズ高速データロガーユニット】
・RD81DL96： シリアル No の上 2 桁が"08"以下
【MELSEC iQ-R シリーズ MES インタフェースユニット】
・RD81MES96N： シリアル No の上 2 桁が"04"以下
【MELSEC iQ-R シリーズ OPC UA サーバユニット】
・RD81OPC96： シリアル No の上 2 桁が"04"以下

ユニットのシリアル No.は、GX Works3 のシステムモニタ(図 1)で確認できます。

1. GX Works3 を起動する。
2. 「メニューバー」から「診断」→「システムモニタ」を選択する。
3. 「システムモニタ」の「製品情報一覧」ボタンを押下する。

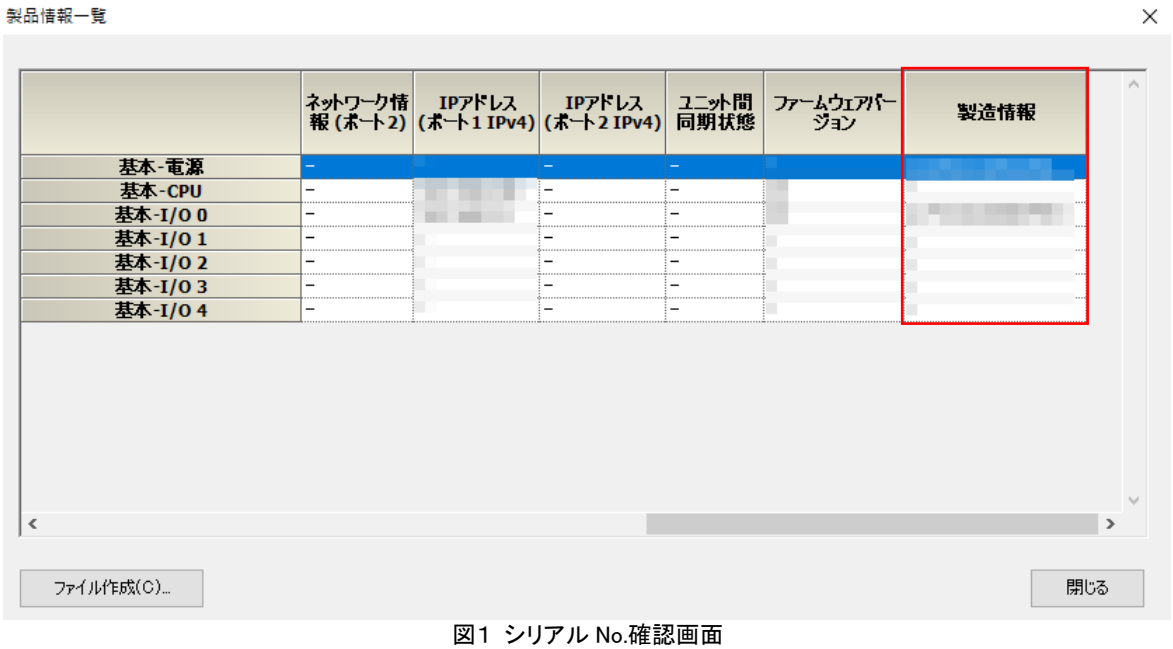

図1 シリアル No.確認画面

■脆弱性の説明

MELSEC iQ-R シリーズ EtherNet/IP ネットワークインタフェースユニット、PROFINET IO コントローラユニット、高速データロガーユニット、MES インタフェースユニットおよび OPC UA サーバユニットは、制御機器等とのデータ送受信を行うために Ethernet 通信ポートを搭載しています。これらのユニットのファームウェア(F/W)に組み込まれている TCP/IP スタックには、以下に示す複数の脆弱性が存在するため、悪意ある第三者の攻撃により、ネットワーク機能を停止、または悪意のあるプログラムを実行される可能性があります。

・バッファエラー(CWE-119) :CVE-2020-5653
・セッションの固定化(CWE-384) :CVE-2020-5654
・NULL ポインタデリファレンス(CWE-476) :CVE-2020-5655
・不適切なアクセス制御(CWE-284) :CVE-2020-5656
・引数の挿入または変更(CWE-88) :CVE-2020-5657
・リソース管理の問題(CWE-399) :CVE-2020-5658

■脆弱性がもたらす脅威

悪意ある第三者によって細工されたパケットを受信した場合、ネットワーク機能が停止する、または悪意あるプログラムを実行される危険性があります。

■対策方法

以下のバージョンで対策を実施しています。

【MELSEC iQ-R シリーズ EtherNet/IP ネットワークインタフェースユニット】
・RJ71EIP91: シリアル No の上 2 桁が"03"以上
【MELSEC iQ-R シリーズ PROFINET IO コントローラユニット】
・RJ71PN92: シリアル No の上 2 桁が"02"以上
【MELSEC iQ-R シリーズ高速データロガーユニット】
・RD81DL96: シリアル No の上 2 桁が"09"以上
【MELSEC iQ-R シリーズ MES インタフェースユニット】
・RD81MES96N: シリアル No の上 2 桁が"05"以上
【MELSEC iQ-R シリーズ OPC UA サーバユニット】
・RD81OPC96: シリアル No の上 2 桁が"05"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やホスト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。