MELSEC iQ-R シリーズの Ethernet ポートにおける サービス拒否(DoS)の脆弱性

公開日 2020 年 11 月 19 日
最終更新日 2021 年 12 月 16 日
三菱電機株式会社

■概要

MELSEC iQ-R シリーズのユニットには、リソース枯渇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。ユニットが攻撃者からの不正な SLMP パケットを受信すると、プログラム実行や通信が DoS 状態に陥る可能性があります。(CVE-2020-5668)

この脆弱性の影響を受ける製品形名およびファームウェアバージョンを以下に示します。

■CVSS スコア

CVE-2020-5668 CVSS:3.0/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

MELSEC iQ-R シリーズのユニットのうち、次の製品形名とファームウェアバージョンのものが影響を受けます。

シリーズ	形名	バージョン
iQ-R シリーズ	R00/01/02CPU	ファームウェアバージョン"19"以前
	R04/08/16/32/120(EN)CPU	ファームウェアバージョン"51"以前
	R08/16/32/120SFCPU	ファームウェアバージョン"22"以前
	R08/16/32/120PCPU	ファームウェアバージョン"25"以前
	R08/16/32/120PSFCPU	ファームウェアバージョン"06"以前
	RJ71EN71	ファームウェアバージョン"47"以前
	RJ71GF11-T2	ファームウェアバージョン"47"以前
	RJ72GF15-T2	ファームウェアバージョン"07"以前
	RJ71GP21-SX	ファームウェアバージョン"47"以前
	RJ71GP21S-SX	ファームウェアバージョン"47"以前
	RJ71GN11-T2	ファームウェアバージョン"11"以前

ユニットのファームウェアバージョンは GX Works3 のシステムモニタにある、下記の製品情報一覧(図 1)より確認できます。
確認方法は、各製品のマニュアルをご参照ください。

	ネットワーク情報(ポート2)	IPアドレス(ポート1 IPv4)	IPアドレス(ポート2 IPv4)	ユニット間同期状態	ファームウェアバージョン	製造情報
基本-電源	-	-	-	-	-	-
基本-CPU	-	-	-	-	51	-
基本-I/O 0	-	-	-	-	-	-
基本-I/O 1	-	-	-	-	-	-
基本-I/O 2	-	-	-	-	-	-
基本-I/O 3	-	-	-	-	-	-
基本-I/O 4	-	-	-	-	-	-
基本-I/O 5	-	-	-	-	-	-
基本-I/O 6	-	-	-	-	-	-
基本-I/O 7	-	-	-	-	-	-

図 1 製品情報一覧

■脆弱性の説明

MELSEC iQ-R シリーズのユニットには、リソース枯渇(CWE-400)によるサービス拒否(DoS)の脆弱性が存在します。

■脆弱性がもたらす脅威

ユニットが攻撃者から不正な SLMP パケットを受信すると、それぞれ以下の状態となる可能性があります。なお, 復旧にはユニットのリセットが必要になります。

① CPU ユニットの場合
エラーが発生し、プログラム実行および通信が DoS 状態に陥る可能性があります。

② CPU ユニット以外の場合
ユニット経由の通信が DoS 状態に陥る可能性があります。

■対策方法

下記ユニットにおいては対策を実施済みです。

シリーズ	形名	バージョン
iQ-R シリーズ	R00/01/02CPU	ファームウェアバージョン"20"以降
	R04/08/16/32/120(EN)CPU	ファームウェアバージョン"52"以降
	R08/16/32/120SFCPU	ファームウェアバージョン"23"以降
	R08/16/32/120PCPU	ファームウェアバージョン"26"以降
	R08/16/32/120PSFCPU	ファームウェアバージョン"07"以降
	RJ71EN71	ファームウェアバージョン"48"以降
	RJ71GF11-T2	ファームウェアバージョン"48"以降
	RJ72GF15-T2	ファームウェアバージョン"08"以降
	RJ71GP21-SX	ファームウェアバージョン"48"以降
	RJ71GP21S-SX	ファームウェアバージョン"48"以降
	RJ71GN11-T2	ファームウェアバージョン"12"以降

■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。

■謝辞

この問題をご報告いただいた国家工業信息安全発展研究中心　張暁菲様に感謝いたします。

■お客様からのお問い合わせ先

お客様からのお問い合わせ先につきましては、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

2021 年 12 月 16 日

RJ71C24(-R2/R4)は本脆弱性に該当しないことが判明したため、該当製品から削除しました。

2021 年 9 月 14 日

RJ71GN11-T2 の対策方法の情報を追加しました。

2021 年 5 月 18 日

R08/16/32/120PCPU および R08/16/32/120PSFCPU の対策方法の情報を追加しました。