MELSEC iQ-R シリーズ CPU ユニットにおける
サービス拒否(DoS)の脆弱性

公開日 2020 年 11 月 12 日
三菱電機株式会社

■概要

MELSEC iQ-R シリーズの CPU 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。攻撃者から不正な HTTP パケットを受信すると、CPU ユニットでエラーが発生し、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。(CVE-2020-5666)

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-2020-5666　CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:N/A:H　　基本値:6.8

■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。

・R00/01/02CPU:ファームウェアバージョン"05"～"19"
・R04/08/16/32/120(EN)CPU:ファームウェアバージョン"35"～"51"

CPU 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画面(図 1)より確認できます。

確認方法の詳細な手順は、以下マニュアルをご参照ください。

・MELSEC iQ-R ユニット構成マニュアル　付 1 製造情報・ファームウェアバージョン 確認方法

	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　製品情報一覧画面

■脆弱性の説明

MELSEC iQ-R シリーズの CPU 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。ただし、エンジニアリングツールで「Web サーバ使用有無」の設定が「使用しない」に設定されている場合、本現象は発生しません(デフォルトは「使用しない」)。

■脆弱性がもたらす脅威

攻撃者から不正な HTTP パケットを受信すると、CPU ユニットでエラーが発生し、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は、対策済みのファームウェアバージョンに更新してください。

・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

■回避策

・Web サーバ機能が不要の場合は、エンジニアリングツールで「Web サーバ使用有無」の設定を「使用しない」に設定してください。設定方法は下記を確認ください。

[設定方法]

Web サーバ設定は，下記の Web サーバ設定画面(図 2)から設定できます。

① [パラメータ]-[CPU ユニット]-[ユニットパラメータ]-[応用設定]-[Web サーバ設定]

② [Web サーバ使用有無]を「使用しない」に設定します。

図 2 Web サーバ設定画面

また、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