MELSEC-Q 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 2025 年 9 月 18 日
三菱電機株式会社

■概要

MELSEC-Q シリーズ CPU ユニットにおいて、ユーザ認証機能が有効になっている場合に、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。中国サイバーセキュリティ法に対応した GX Works2 で設定を行った時のみユーザ認証機能がデフォルトで有効になり、通常ではユーザ認証機能が無効になっています。攻撃者は、当該製品に対して細工した不正なパケットを送信することにより、整数アンダーフローを発生させ、当該製品の Ethernet 通信及び制御プログラム実行を停止させることができる可能性があります。(CVE-2025-8531)

■CVSS スコア [1]

CVE-2025-8531　CVSS:3.1/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

影響を受ける製品とバージョンは以下の通りです。

シリーズ	形名	バージョン
MELSEC-Q シリーズ	Q03/04/06/13/26UDVCPU	シリアル No.の上 5 桁"24082"以降～"27081"以前
	Q04/06/13/26UDPVCPU	シリアル No.の上 5 桁"24082"以降～"27081"以前

■脆弱性の説明

MELSEC-Q シリーズ CPU ユニットにおいて、ユーザ認証機能が有効になっている場合に、レングスパラメーターの不整合による不適切な処理(CWE-130[2])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

攻撃者は、当該製品に対して細工した不正なパケットを送信することにより、整数アンダーフローを発生させ、当該製品の Ethernet 通信及び制御プログラム実行を停止させることができる可能性があります。なお、復旧には当該製品のリセットが必要になります。

■お客様での対応

該当製品・該当バージョンをご使用のお客様は、軽減策・回避策にて対応ください。

「■製品での対応」のとおり対策済み製品をリリースしておりますが、対策版へのアップデートはできません。後継機種である MELSEC iQ-R シリーズへの移行もご検討ください。

■製品での対応

対策済の製品およびバージョンは、以下となります。

シリーズ	形名	バージョン
MELSEC-Q シリーズ	Q03/04/06/13/26UDVCPU	シリアル No.の上 5 桁"27082"以降
	Q04/06/13/26UDPVCPU	シリアル No.の上 5 桁"27082"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。

・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。
・当該製品並びに当該製品へ接続可能なパソコン及びネットワーク機器への物理的なアクセスを制限してください。

■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

1 https://www.ipa.go.jp/security/vuln/scap/cvssv3.html
2 https://cwe.mitre.org/data/definitions/130.html