FA 製品の当社専用プロトコル通信及び SLMP 通信における情報漏えい、情報改ざん及びサービス拒否(DoS)の脆弱性

公開日 2026 年 2 月 5 日
三菱電機株式会社

■概要
FA 製品で使用されている当社専用プロトコル通信及び SLMP 通信において、情報漏えい、情報改ざん及びサービス拒否(DoS)の脆弱性が存在することが判明しました。攻撃者は、該当製品に対して特定のコマンドを含んだ不正なパケットを送信することにより、該当製品において制御プログラムの一部やデバイスデータを読み出す、デバイスデータを書き込む又は該当製品をサービス停止(DoS)状態に陥らせることができる可能性があります。(CVE-2025-15080)

■CVSS スコア [1]
CVE-2025-15080 CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:H/VA:H/SC:N/SI:N/SA:N 基本値 8.8

■該当製品の確認方法
影響を受ける製品は以下の製品です。

シリーズ	製品形名	バージョン
MELSEC-iQ R シリーズ	R08/16/32/120PCPU	48 以前

■脆弱性の説明
該当製品における当社専用プロトコル通信及び SLMP 通信の特定のコマンドには、入力で指定された数量の不適切な検証(CWE-1284[2])に起因する情報漏えい、情報改ざん及びサービス拒否(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、該当製品に対して特定のコマンドを含んだ不正なパケットを送信することにより、該当製品において制御プログラムの一部やデバイスデータを読み出す、デバイスデータを書き込む又は該当製品をサービス停止(DoS)状態に陥らせることができる可能性があります。

■お客様での対応
該当製品をご使用のお客様は、以下に示す手順に従って、ファームウェアを「■製品での対応」に記載の対策済みのバージョンに更新してください。

【更新手順】
以下のサイトから、「■製品での対応」に記載の対策済みバージョンのアップデートファイル、ファームウェアバージョンアップ用エンジニアリングソフトウェア及びマニュアルをダウンロードしたうえで、アップデートしてください。
https://www.mitsubishielectric.co.jp/fa/download/index.html
アップデートの方法は、以下を参照ください。
・MELSEC iQ-R ユニット構成マニュアル 「付 2 ファームウェアアップデート機能」

■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	製品形名	バージョン
MELSEC-iQ R シリーズ	R08/16/32/120PCPU	49 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。
・ファイアウォール、IP フィルタ機能などを使用し、当該製品への接続を最小限に抑え、信頼できないネットワークやホストからアクセスできないようにしてください。IP フィルタ機能については、以下のマニュアルを参照ください。
MELSEC iQ-R Ethernet ユーザーズマニュアル(応用編)の「1.13 セキュリティ」の「IP フィルタ」
・当該製品および当該製品が接続された LAN への物理的なアクセスを制限してください。

1 https://www.first.org/cvss/v4-0/specification-document
2 https://cwe.mitre.org/data/definitions/1284.html

■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