MELSOFT 交信ポート(UDP/IP)におけるリモートアクセスの脆弱性

公開日 2020 年 3 月 30 日
三菱電機株式会社

■概要
MELSEC iQ-R, iQ-F, Q, L, F シリーズの MELSOFT 交信ポート(UDP/IP)には, リソース枯渇(CWE-400)の脆弱性が存在することが判明しました。攻撃者が該当製品の MELSOFT 交信ポート(UDP/IP)に, 大量のデータを送信すると, MELSOFT 交信ポート(UDP/IP)が処理不能状態に陥る場合があります。

■該当製品の確認方法
影響を受ける製品は, MELSEC iQ-R, iQ-F, Q, L, F シリーズの Ethernet ポートにて MELSOFT 交信ポート(UDP/IP)を持つユニットです。全てのバージョンが該当します。

■脆弱性の説明
三菱電機株式会社が提供する MELSEC iQ-R, iQ-F, Q, L, F シリーズの MELSOFT 交信ポート(UDP/IP)には, リソースの枯渇(CWE-400)の脆弱性が存在します。

■脆弱性がもたらす脅威
MELSOFT 交信ポートが処理不能状態に陥った場合, 正常なクライアントが MELSOFT 交信ポートに接続できなくなり, 他の交信ポートで通信している機器が繋がりにくくなります。なお, 本脆弱性により, Ethernet 通信以外の機能が影響を受けることはありません。

■お客様での対応
インターネット経由の外部機器からの不正アクセスに対しては, 弊社マニュアル*1 の【設計上の注意事項】に, 「警告」としてご案内しておりますとおり, 弊社シーケンサシステムの安全を保つ必要があるときは, ファイアウォールなどの対策を盛り込んでください。
*1 例)MELSEC iQ-R Ethernet ユーザーズマニュアル(応用編)
また, 以下のいずれか, または組み合わせて実施いただくことで, 本脆弱性による被害を軽減/防止することができます。

1. ファイアウォールを設置する。
2. IP フィルタ機能を使用し, 接続可能な IP アドレスを制限する。

■謝辞
この問題をご報告いただいた Rongkuan Ma 様, Jie Meng 様, Peng Cheng 様に感謝いたします。

■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。