MELSEC iQ-R、iQ-F、Q、L、FX シリーズの CPU ユニットと GX Works3 および GX Works2 間の通信に、情報漏えい、情報改ざん、不正操作、サービス拒否(DoS)の脆弱性

公開日 2020 年 6 月 23 日
三菱電機株式会社

■概要
MELSEC iQ-R、iQ-F、Q、L、FX シリーズの CPU ユニットと GX Works3 および GX Works2 間の通信は平文で行われるため、情報漏えい、情報改ざん、不正操作、サービス拒否（DoS）の脆弱性があります(CWE-319)。信頼できないネットワークやホストを経由した通信を行った場合、悪意のある攻撃者により、通信データの盗聴・改ざん、不正な操作及びサービス妨害(DoS)攻撃を受けるリスクがあります。

■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、FX シリーズの CPU 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
MELSEC iQ-R、iQ-F、Q、L、FX シリーズの CPU ユニットと GX Works3 及び GX Works2 間の通信は、平文で行われるため、情報漏えい、情報改ざん、不正操作、サービス拒否(DoS)の脆弱性(CVE-2020-5594)があります(CWE-319)。

■脆弱性がもたらす脅威
悪意のある攻撃者により、情報漏えい、情報改ざん、不正な操作及びサービス妨害(DoS)攻撃が行われる可能性があります。

■お客様での対応
信頼できないネットワークやホストを経由した通信を行う場合は、VPN の設置により通信経路を暗号化することで、本脆弱性の影響を軽減できます。

■謝辞
この問題をご報告いただいた浙江大学 NESC ラボ Shunkai Zhu 様、Rongkuan Ma 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。