MELSOFT 交信ポート(TCP/IP)におけるサービス拒否(DoS)の脆弱性

公開日 2021 年 5 月 27 日
三菱電機株式会社

■概要
MELSEC iQ-R シリーズ CPU ユニットの MELSOFT 交信ポート(TCP/IP)には，セッション管理の不備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。攻撃者はコネクションを適切に閉じないことでリソース枯渇を発生させ、当該機器を DoS 状態に陥らせることができます。(CVE-2021-20591)
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-2021-20591　CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L　基本値:5.3

■該当製品の確認方法
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。

形名	ファームウェアバージョン
R00/01/02CPU	全バージョン
R04/08/16/32/120(EN)CPU	全バージョン
R08/16/32/120SFCPU	全バージョン
R08/16/32/120PCPU	全バージョン
R08/16/32/120PSFCPU	全バージョン

■脆弱性の説明
MELSEC iQ-R シリーズ CPU ユニットの MELSOFT 交信ポート(TCP/IP)には，リソースの枯渇(CWE-400) 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
攻撃者が MELSOFT 交信ポート(TCP/IP)に接続したままの状態とすることで，正規のユーザが MELSOFT 交信ポート(TCP/IP)に接続できなくなります。
・複数の MELSOFT 交信ポート(TCP/IP ポート)をオープンしている場合，他ポートへの影響はありません。
・シーケンス制御への影響はありません。

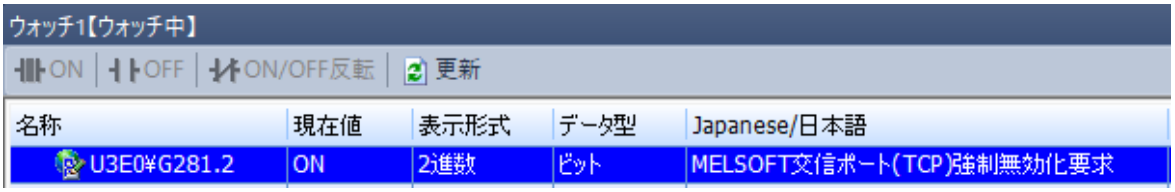
■対策方法
下記軽減策・回避策にて対応ください。

サービス拒否(DoS)の状態になった場合には、コネクション強制無効化機能によって当該ポートを強制的に無効化した後、再度有効化することで，正規のユーザが接続可能となります。
例として iQ-R シリーズ CPU ユニットの場合の該当マニュアル ※1の抜粋と設定方法を示します。
※1:MELSEC iQ-R Ethernet ユーザーズマニュアル(応用編) 付 3 バッファメモリ
＜例＞
・マニュアル抜粋

■コネクション強制無効化 システムポート(Un￥G281)

アドレス	内容
Un￥G281	強制的に無効にしたいシステムポートを設定します。 0:許可 1:拒否 各システムポートに対応したビットは下記のとおりです。 b0:自動オープンUDPポート b1:MELSOFT交信ポート(UDP/IP) b2:MELSOFT交信ポート(TCP/IP) b3:FTP交信用ポート b4:MELSOFTの直結接続

・設定方法
ウォッチ，またはデバイス/バッファメモリ一括モニタにて，b2 に「ON」を設定してください。その後、再度「OFF」を設定することで、正規のユーザが接続可能となります。
＜例:ウォッチの場合＞



■軽減策・回避策

＜軽減策＞

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のいずれか，または組み合わせての対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。

・IP フィルタ機能 ※2を使用し，接続可能な IP アドレスを適切に制限してください。

・MELSOFT 交信ポート(UDP/IP)を使用してください。

※2：MELSEC iQ-R Ethernet ユーザーズマニュアル(応用編) 1.13 セキュリティの「IP フィルタ」を参照ください。

＜回避策＞

MELSOFT 交信ポート(TCP/IP)の 5007 ポートの機能が不要な場合は、予め対策方法に記載のコネクション強制無効化機能にて、b2 に「1」を設定してください。

■謝辞

この問題をご報告いただいた Nozomi Networks 社 Younes Dragoni 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