GOT の MODBUS/TCP スレーブ通信機能における サービス拒否(DoS)の脆弱性

公開日 2021 年 7 月 27 日
三菱電機株式会社

■概要

GOT2000 シリーズ及び GT SoftGOT2000 の MODBUS/TCP スレーブ通信機能において、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。攻撃者によって GOT の MODBUS/TCP 通信用ポートに対して接続、通信、切断を高速に繰り返し実行された場合、当該機器の通信機能が停止する可能性があります。(CVE-2021-20592)

■CVSS スコア

CVE-2021-20592　CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H　基本値:5.9

■該当製品の確認方法

【該当製品およびバージョン】

影響を受ける製品とバージョンは以下の通りです。

GOT2000 シリーズで「MODBUS/TCP スレーブ,ゲートウェイ」通信ドライバをご使用の場合

シリーズ	モデル	該当通信ドライバのバージョン
GOT2000	GT27 モデル	01.19.000 ～ 01.39.010
	GT25 モデル	01.19.000 ～ 01.39.010
	GT23 モデル	01.19.000 ～ 01.39.010

GT SoftGOT2000 で接続設定の機種に「MODBUS/TCP Slave」を選択してご使用の場合

シリーズ	モデル	該当ソフトウェアバージョン
GT SoftGOT2000	—	1.170C ～ 1.256S

【バージョン確認方法】

バージョン確認方法については、以下のマニュアルを参照してください。

なお、最新のマニュアルについては、三菱電機 FA サイト(https://www.mitsubishielectric.co.jp/fa/)のマニュアルダウンロードコーナーよりダウンロードできます。

GOT2000 シリーズの場合

GOT2000 シリーズ本体取扱説明書(ユーティリティ編)(SH-081187)

「6.9 章パッケージ管理」内の「プロパティ操作」

GT SoftGOT2000 の場合

GT SoftGOT2000 Version1 操作マニュアル (SH-081193)

「2.7 章ヘルプ」内の「GT SoftGOT2000 のバージョン確認手順([バージョン情報]選択時)」

■脆弱性の説明

GOT2000 シリーズの「MODBUS/TCP スレーブ,ゲートウェイ」通信ドライバをご使用の場合及び GT SoftGOT2000 で接続設定の機種に「MODBUS/TCP Slave」を選択してご使用の場合において、共有リソースへのアクセス同期不備(CWE-820)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

攻撃者によって GOT の MODBUS/TCP 通信用ポートに対して接続、通信、切断を高速に繰り返し実行された場合、当該機器の通信機能が停止する可能性があります。

その場合、復旧するには下記の処置を実施してください。

GOT2000 シリーズは、電源再投入、又は、リセットスイッチの押下による再起動をしてください。

GT SoftGOT2000 は、ソフトウェアが強制終了するため、再度起動してください。

■対策方法

該当製品/バージョンの「MODBUS/TCP スレーブ,ゲートウェイ」通信ドライバ及び「MODBUS/TCP Slave」をご使用のお客様は、以下に示す手順に従って対策バージョンに更新してください。

【対策バージョン】

GOT2000 シリーズで「MODBUS/TCP スレーブ,ゲートウェイ」通信ドライバをご使用の場合
(GT Designer3 Version1(GOT2000) Ver.1.260W 以降に同梱されています。)

シリーズ	モデル	該当通信ドライバの対策バージョン
GOT2000	GT27 モデル	01.40.000 以降
	GT25 モデル	01.40.000 以降
	GT23 モデル	01.40.000 以降

GT SoftGOT2000 で接続設定の機種に「MODBUS/TCP Slave」を選択してご使用の場合

シリーズ	モデル	該当ソフトウェアの対策バージョン
GT SoftGOT2000	—	1.260W 以降

【更新手順】

GOT2000 シリーズの場合

① 三菱電機 FA サイト(https://www.mitsubishielectric.co.jp/fa/)のソフトウェアダウンロードコーナーより、最新の GT Designer3 Version1(GOT2000)をダウンロードし、インストーラのメッセージに従いパソコンにインストールしてください。
② 該当製品で使用しているプロジェクトデータを GT Designer3 Version1(GOT2000)で開きます。
③ [通信]→[GOT への書込み]メニューを選択し、パッケージデータを GOT 本体へ転送してください。転送に関する詳細な手順は、以下のマニュアルを参照してください。なお、最新のマニュアルについては、三菱電機 FA サイト(https://www.mitsubishielectric.co.jp/fa/)のマニュアルダウンロードコーナーよりダウンロードできます。
GT Designer3 (GOT2000) 画面設計マニュアル(SH-081219)
「4 章 GOT と通信する」
④ 前述のバージョン確認方法に従い、対策バージョンとなっていることを確認してください。

GT SoftGOT2000 の場合

① 三菱電機 FA サイト(https://www.mitsubishielectric.co.jp/fa/)のソフトウェアダウンロードコーナーより、最新の GT SoftGOT2000 Version1 をダウンロードし、インストーラのメッセージに従いパソコンにインストールしてください。
② 前述のバージョン確認方法に従い、対策バージョンとなっていることを確認してください。

■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を講じることを推奨します。
(1)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。
(2)LAN 内で使用し、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。
(3)該当製品へアクセス可能なパソコンにウイルス対策ソフトを搭載してください。

■謝辞

この問題をご報告いただいた COE-CNDS Lab, VJTI, Mumbai, India の Parul Sindhwad 様と Dr. Faruk Kazi 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弊社の支社、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

■登録商標