GOT およびテンションコントローラの 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 5 月 11 日
最終更新日 2022 年 1 月 20 日
三菱電機株式会社

■概要

GOT2000 シリーズ、GOT SIMPLE シリーズ GS21 モデル及び GT SoftGOT2000、並びにテンションコントローラの 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。攻撃者から不正なパケットを受信した場合、当該機器の通信機能が停止する可能性があります。(CVE-2021-20589)

■CVSS スコア

CVE-2021-20589　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。

(1)表示器:GOT

「MODBUS/TCP スレーブ, ゲートウェイ」通信ドライバをご使用している場合、該当となります。

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 ～ 01.38.000
	GT25 モデル	01.19.000 ～ 01.38.000
	GT23 モデル	01.19.000 ～ 01.38.000
	GT21 モデル	01.21.000 ～ 01.39.000
GOT SIMPLE	GS21 モデル	01.21.000 ～ 01.39.000
GT SoftGOT2000	—	1.170C ～ 1.250L

表示器:GOT におけるバージョン確認方法

「MODBUS/TCP スレーブ, ゲートウェイ」通信ドライバの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。

GT27/GT25/GT23 モデルの場合

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」

GT21/GS21 モデルの場合

GOT2000 シリーズ本体取扱説明書(ユーティリティ編)(SH-081187)
「15.2 章 OS 情報」

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)」

(2)テンションコントローラ

下記テンションコントローラにおいて、MODBUS/TCP 通信用画面パッケージデータを使用している場合、該当となります。

形名	画面パッケージデータ名	画面パッケージデータのバージョン
LE7-40GU-L	LE7-40GU-L MODBUS/TCP 通信用画面パッケージデータ	V1.00

テンションコントローラにおけるバージョン確認方法

テンションコントローラの「画面番号 961:本体 ROM・画面バージョン」の画面にて画面バージョンをご確認ください。

上記画面の表示方法及び操作方法につきまし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。

LE7-40GU-L 取扱説明書(活用編)(SH-170021)

■脆弱性の説明

GOT2000 シリーズ、GOT SIMPLE シリーズ GS21 モデル及び GT SoftGOT2000、並びにテンションコントローラの MODBUS/TCP スレーブ通信機能において、不適切な長さの値によるバッファへのアクセス（CWE-805）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

攻撃者から不正なパケットを受信した場合、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。

(1)表示器：GOT

GOT の電源再投入、又は、リセットスイッチの押下による再起動が必要です(リセットスイッチは、GT27/25/23 モデルのみ搭載)。GT SoftGOT2000 は、ソフトウェアが強制終了するため、再度起動する必要があります。

(2)テンションコントローラ

テンションコントローラ本体の電源再投入を行ってください。

■対策方法

(1)表示器：GOT

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】

「MODBUS/TCP スレーブ，ゲートウェイ」通信ドライバの対策バージョンは以下の通りです。
（GT Designer3 Version1(GOT2000) Ver.1.255R 以降のバージョン）

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	01.39.000 以降
	GT25 モデル	01.39.000 以降
	GT23 モデル	01.39.000 以降
	GT21 モデル	01.40.000 以降
GOT SIMPLE	GS21 モデル	01.40.000 以降
GT SoftGOT2000	—	1.255R 以降

【更新手順】

GOT2000 シリーズ、GOT SIMPLE 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 前述の表示器：GOT における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 前述の表示器：GOT における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。

(2)テンションコントローラ

該当製品/バージョン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】

画面パッケージデータの対策バージョンは以下の通りです。

形名	画面パッケージデータ名	画面パッケージデータの対策バージョン
LE7-40GU-L	LE7-40GU-L MODBUS/TCP 通信用画面パッケージデータ	V1.01 以降

【更新手順】

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、対策バージョンの画面パッケージデータをダウンロードしてください。
② 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、最新のエンジアリングツール(「データ転送ツール」または「GT Designer 3 Version1(GOT2000)」)をパソコンにインストールしてください。
③ USB ケーブルで LE7-40GU-L の USB インタフェースとパソコンを接続してください。
④ エンジアリングツールの「GOT 書込」機能で画面パッケージデータを LE7-40GU-L に書き込んでください。
⑤ エンジアリング上で画面書込み完了のダイアログが表示されたら、LE7-40GU-L を再起動してください。
⑥ 前述のテンションコントローラにおける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

(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

■更新履歴

2022 年 1 月 20 日
テンションコントローラの対策方法の情報を追加しました。