GOT2000 シリーズ、GOT SIMPLE シリーズ、GT SoftGOT2000 における情報改ざんの脆弱性

公開日 2021 年 11 月 16 日
三菱電機株式会社

■概要

GOT2000 シリーズ、GOT SIMPLE シリーズ、GT SoftGOT2000 には、デバイス値に対する不適切な入力確認(CWE-20)による、情報改ざんの脆弱性が存在することが判明しました。攻撃者が悪意をもったパケットを送信し、デバイス値の書き換えを行った場合に、設定された入力範囲の制限を超える値が、書き込まれる可能性があります。（CVE-2021-20601）

■CVSS スコア

CVE-2021-20601　CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N　基本値:7.5

■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。

シリーズ	モデル	バージョン
GOT2000	GT27 モデル	全バージョン
	GT25 モデル	全バージョン
	GT23 モデル	全バージョン
	GT21 モデル	全バージョン
GOT SIMPLE	GS21 モデル	全バージョン

シリーズ	モデル	ソフトウェアバージョン
GT SoftGOT2000	—	全バージョン

■脆弱性の説明

GOT2000 シリーズ、GOT SIMPLE シリーズ、GT SoftGOT2000 には、不適切な入力確認(CWE-20)による、情報改ざんの脆弱性が存在します。

■脆弱性がもたらす脅威

攻撃者が悪意をもったパケットを送信し、デバイス値の書き換えを行った場合に、設定された入力範囲の制限を超える値が、書き込まれる可能性があります。その結果、システムが誤動作するなど、システムの動作に影響を与える可能性があります。

弊社マニュアル※1 の注意事項でご案内しておりますとおり、入力範囲の設定は、当該製品の GUI から入力を行った場合のみ有効です。ネットワーク経由での外部機器からの入力に対しては、本設定は有効に機能しません。

※1：GT Designer3 (GOT2000)画面設計マニュアル(SH-081219)「8.4.3 章 数値表示、数値入力の注意事項」

■対策方法

軽減策を実施ください。

■軽減策

ネットワーク経由による外部機器からの不正アクセスに対して、弊社の GOT およびシステムの安全を保つ必要があるときは、弊社マニュアル※2 の【設計上の注意事項】にてご案内しておりますとおり、ファイアウォールなどの対策を盛り込んでください。

※2：例) GT Designer3 (GOT2000) 画面設計マニュアル(SH-081219)「設計上の注意事項」

具体的には以下のいずれか、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)当該製品やシステム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)当該製品やシステム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。

(4)IP フィルタ機能※3 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。

※3：GT Designer3 (GOT2000)画面設計マニュアル(SH-081219)「5.4.3 章 IP フィルタを設定する」

■謝辞

この問題および弊社製品の改善点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