

GOT の VNC サーバ機能におけるパスワード認証回避の脆弱性

公開日 2021 年 4 月 22 日

最終更新日 2021 年 7 月 27 日

三菱電機株式会社

■概要

GOT2000 シリーズ、GOT SIMPLE シリーズの VNC サーバ機能において、VNC サーバ接続時のパスワード認証が回避される脆弱性が存在することが判明しました。当該製品は、VNC サーバの設定が有効になっている場合に、攻撃者から不正なパケットを受信すると、VNC サーバに不正アクセスされる可能性があります。(CVE-2021-20590)

■CVSS スコア

CVE-2021-20590 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N 基本値:5.9

■該当製品の確認方法

影響を受ける製品とバージョンは以下の通りです。

「VNC サーバ」機能をご使用している場合、該当となります。

シリーズ	モデル	形名	VNC サーバのバージョン
GOT2000	GT27 モデル	全て	01.39.010 以前
	GT25 モデル	全て	01.39.010 以前
	GT21 モデル	GT2107-WTBD	01.40.000 以前
		GT2107-WTSD	
GOT SIMPLE	GS21 モデル	GS2110-WTBD-N	01.40.000 以前
		GS2107-WTBD-N	

【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。

GT27/25 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」

■脆弱性の説明

GOT の VNC サーバ機能には、不適切な認証(CWE-287)によるパスワード認証回避の脆弱性が存在します。

■脆弱性がもたらす脅威

GOT2000 シリーズ、GOT SIMPLE シリーズの VNC サーバ機能にて、VNC サーバ接続時のパスワード認証が回避される脆弱性が存在します。

当該製品は、VNC サーバの設定が有効になっている場合に、攻撃者から不正なパケットを受信すると、VNC サーバに不正アクセスされる可能性があります。

■対策方法

該当製品/バージョンの「VNC サーバ」機能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】

「VNC サーバ」機能の対策バージョンは以下の通りです。

(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	形名	VNC サーバの対策バージョン
GOT2000	GT27 モデル	全て	01.40.000 以降
	GT25 モデル	全て	01.40.000 以降
	GT21 モデル	GT2107-WTBD GT2107-WTSD	01.41.000 以降
GOT SIMPLE	GS21 モデル	GS2110-WTBD-N	01.41.000 以降
		GS2107-WTBD-N	

【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、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 への書き込み]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。

■軽減策

製品への VNC によるアクセスを、信頼できるネットワークやホストからのアクセスに制限してください。

■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

VNC は、RealVNC Ltd. の米国およびその他の国における登録商標です。

■更新履歴

2021 年 7 月 27 日

該当製品の確認方法および対策方法の情報を追加しました。