GOT2000 シリーズおよび GOT SIMPLE シリーズの FTP サーバ機能における なりすましおよびサービス拒否(DoS)の脆弱性

公開日 2023 年 8 月 3 日
三菱電機株式会社

■概要

GOT2000 シリーズおよび GOT SIMPLE シリーズの FTP サーバ機能にはデータコネクションのポート番号が容易に推測可能であるため、なりすまし(データコネクションのセッションハイジャック)およびサービス拒否(DoS)の脆弱性が存在することが、判明しました。攻撃者が、FTP サーバのデータコネクションの待受けポートを推測して接続することにより、データコネクションを横取り(セッションハイジャック)したり、正規ユーザによるデータコネクションの確立を妨げる(DoS 状態に陥らせる)可能性があります。データコネクションを横取りされることにより、該当製品のデータが窃取されたり、改ざんされる可能性があります。(CVE-2023-3373)

■CVSS スコア [1]

CVE-2023-3373　CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:L　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とおりです。

FTP サーバ機能をご使用している場合に該当となります。

シリーズ	モデル	基本システムアプリケーションのバージョン
GOT2000	GT21 モデル	01.49.000 以前
GOT SIMPLE	GS21 モデル	01.49.000 以前

【バージョン確認方法】

バージョンの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。

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

GOT2000 シリーズおよび GOT SIMPLE シリーズの FTP サーバ機能には、過去の値から予測可能な値の使用(CWE-342) [2]により、データコネクションのポート番号が容易に推測可能であるため、なりすまし(データコネクションのセッションハイジャック)およびサービス拒否(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、FTP サーバのデータコネクションの待受けポートを推測して接続することにより、データコネクションを横取り(セッションハイジャック)したり、正規ユーザによるデータコネクションの確立を妨げる(DoS 状態に陥らせる)可能性があります。データコネクションを横取りされることにより、該当製品のデータが窃取されたり、改ざん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 FTP 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】

(GT Designer3 Version1(GOT2000) Ver.1.300N 以降に同梱されています。)

シリーズ	モデル	基本システムアプリケーションの対策バージョン
GOT2000	GT21 モデル	01.50.000 以降
GOT SIMPLE	GS21 モデル	01.50.000 以降

1 https://www.ipa.go.jp/security/vuln/CVSSv3.html
2 https://cwe.mitre.org/data/definitions/342.html

【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・回避策

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・回避策を講じることを推奨します。

【軽減策】

・当該製品および当該製品が接続された LAN への物理的なアクセスを制限してください。
・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。
・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。
・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。
・IP フィルタ機能※1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。

※1: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」を参照ください。

【回避策】

・FTP サーバ機能の要否を見直し、不要な場合には FTP サーバ機能を無効にしてください。

■お問い合わせ先

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