GT Designer3 における情報漏えいの脆弱性

公開日 2025 年 12 月 16 日
三菱電機株式会社

■概要
GT Designer3 において、重要な情報の平文保存(CWE-312[1])に起因する情報漏えいの脆弱性が存在することが判明しました。GT Designer3 は認証情報を平文で保存し、平文のままで認証情報の突合を行っており、攻撃者は、GT Designer3 のプロジェクトデータから平文で保存された認証情報を取得することができます。結果として、攻撃者は、取得した認証情報を用いて、GOT2000 シリーズ又は GOT1000 シリーズを不正に操作することができる可能性があります。(CVE-2025-11009)

■CVSS スコア [2]
CVE-2025-11009　CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N 基本値:5.1

■該当製品
影響を受ける製品及びバージョンは以下のとおりです。
GT Designer3 Version1 (GOT2000) 全バージョン
GT Designer3 Version1 (GOT1000) 全バージョン

■脆弱性の説明
GT Designer3 には、重要な情報の平文保存(CWE-312)に起因する情報漏えいの脆弱性が存在します。

■脆弱性がもたらす脅威
攻撃者は、GT Designer3 のプロジェクトデータから平文で保存された認証情報を取得することができます。結果として、攻撃者は、取得した認証情報を用いて、GOT2000 シリーズ又は GOT1000 シリーズを不正に操作することができる可能性があります。

■お客様での対応
対策版のリリース予定はございませんので、軽減策・回避策にて対応をお願いいたします。

■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を講じることを推奨します。
・該当製品を使用する PC を LAN 内で使用し、信頼できないネットワークやホスト、ユーザからのリモートログインをブロックしてください。
・該当製品をインストールされた PC 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)等で不正アクセスを防止したうえで、信頼できるユーザのみにリモートログインを許可してください。
・該当製品がインストールされた PC 並びに同 PC と通信可能な PC 及びネットワーク機器への物理的なアクセスを制限してください。
・該当製品を使用する PC にウイルス対策ソフトを搭載してください。
・信頼できないファイルを開いたり、信頼できないリンクをクリックしないでください。

■謝辞
この問題をご報告いただいた、NSHC Red Alert Lab の Hea-Eun Moon 様及び Junbeom Gwak 様に感謝いたします。

■お客様からのお問い合わせ先
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

1 https://cwe.mitre.org/data/definitions/312.html
2 https://www.ipa.go.jp/security/vuln/CVSSv3.html