GT SoftGOT2000 における
OpenSSL に起因する悪意のあるコマンドが実行される脆弱性

公開日 2022 年 11 月 15 日
三菱電機株式会社

■概要

GT SoftGOT2000 に搭載している OpenSSL に悪意のあるコマンドが実行される脆弱性が存在することが判明しました。攻撃者は、細工した証明書を送信することにより、悪意のある OS コマンドを実行することができます。(CVE-2022-2068)

■CVSS スコア

CVE-2022-2068　CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H　基本値:9.8

■該当製品の確認方法

影響を受ける製品は以下の通りです。

製品	該当ソフトウェアバージョン
GT SoftGOT2000	1.275M ～ 1.280S

【バージョン確認方法】

1. GT SoftGOT2000 を実行します。
2. メニューの[ヘルプ] -> [バージョン情報]を選択します。
3. [バージョン情報]画面が表示されるので、バージョンを確認します(図 1 参照)。

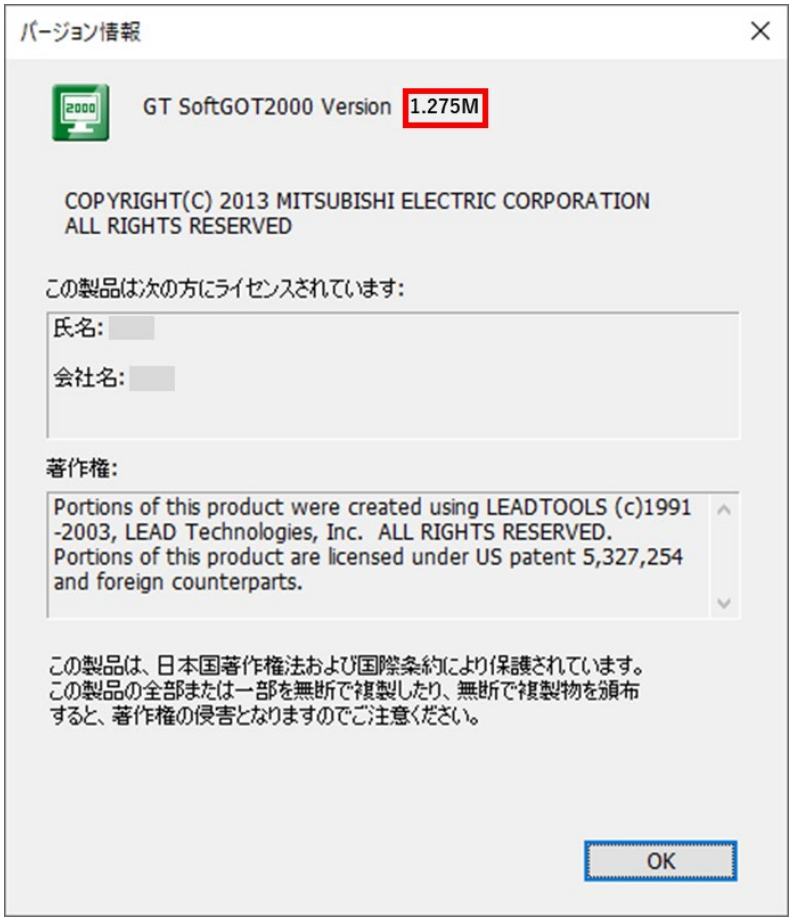

図 1 GT SoftGOT2000 バージョン情報画面

■脆弱性の説明

GT SoftGOT2000に搭載しているOpenSSLには、以下の欠陥を起因とする悪意のあるOSコマンドが実行される脆弱性(CVE-2022-2068)が存在します。

・CVE-2022-2068：OS コマンドインジェクション(CWE-78)

■脆弱性がもたらす脅威

攻撃者は、細工した証明書を送信することにより、当該製品に対し、悪意のあるコマンドを実行することができます。

■対策方法

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】

製品	該当ソフトウェアの対策バージョン
GT SoftGOT2000	1.285X 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、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。
詳細なインストール手順については「GT SoftGOT2000 Version1 操作マニュアル(SH-081193)」を参照ください。

(2) 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を講じることを推奨します。

・当該製品を LAN 内で使用し、信頼できないネットワークやホストとの通信をファイアウォールでブロックしてください。
・当該製品を使用するパソコンにウイルス対策ソフトを搭載してください。
・当該製品を使用するパソコンおよび同一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。
・信頼できない証明書を保存しないでください。
・信頼できない送信元からのメール等に記載された Web リンクをクリックしないでください。

■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