

MELSOFT GT OPC UA Client における OpenSSL の脆弱性に起因する 情報漏えい及びサービス拒否(DoS)の脆弱性

公開日 2022 年 5 月 10 日
三菱電機株式会社

■概要

MELSOFT GT OPC UA Client において、OpenSSL での境界外読み取り及び整数オーバーフロー(ラウンドアップ)による、情報漏えい及びサービス拒否(DoS)の脆弱性が存在することが判明しました。当該製品は、GT SoftGOT2000 と連携し、OPC UA サーバとの通信の機能を GT SoftGOT2000 に提供します。細工したメッセージを送信するなど、何等かの方法で、悪意のある攻撃者にこれらの脆弱性を悪用されることにより、GT SoftGOT2000 においてメモリ上の情報が漏えいしたり、GT SoftGOT2000 がサービス停止(DoS)状態に陥る可能性があります。(CVE-2021-3712、CVE-2021-23840)

■CVSS スコア

CVE-2021-3712 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H 基本値:7.4
CVE-2021-23840 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H 基本値:7.5

■該当製品の確認方法

以下の製品の組み合わせで GT SoftGOT2000 が「OPC UA クライアント接続」をしている場合、該当となります。

【該当製品およびバージョン】

該当製品とバージョンは以下の通りです。

製品	該当ソフトウェアバージョン
MELSOFT GT OPC UA Client	1.00A～1.02C

【組み合わせの対象となる製品およびバージョン】

組み合わせの対象となる製品とバージョンは以下の通りです。

製品	該当ソフトウェアバージョン
GT SoftGOT2000	1.215Z～1.270G

【バージョン確認方法】

MELSOFT GT OPC UA Client の場合

1. MELSOFT GT OPC UA Client 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)。

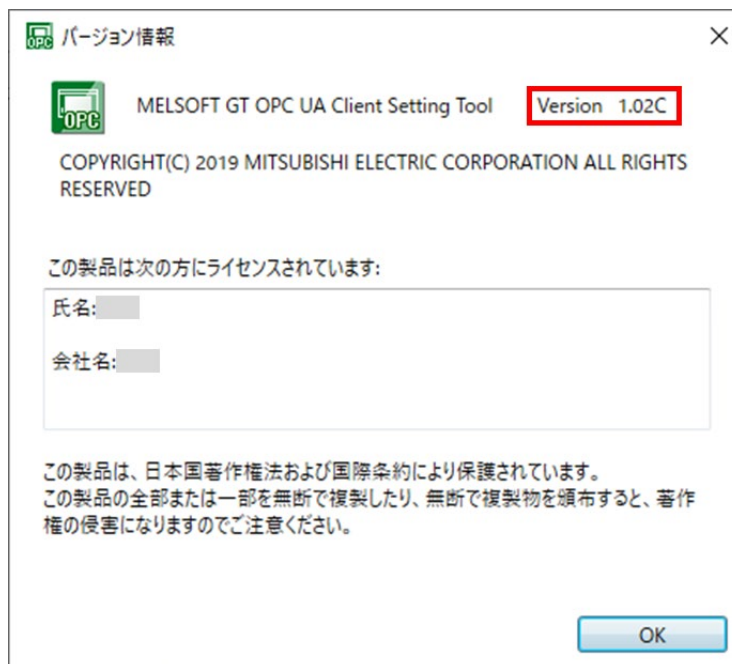


図 1 MELSOFT GT OPC UA Client

GT SoftGOT2000 の場合

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 2 参照)。



図 2 GT SoftGOT2000

■脆弱性の説明

MELSOFT GT OPC UA Client において、OpenSSL での境界外読み取り及び整数オーバーフロー(ラウンドアップ)による、情報漏えい及びサービス拒否(DoS)の脆弱性が存在します。

- ・CVE-2021-3712: 境界外読み取り(CWE-125)
- ・CVE-2021-23840: 整数オーバーフローまたはラップアラウンド(CWE-190)

■脆弱性がもたらす脅威

細工したメッセージを送信するなど、何等かの方法で、悪意のある攻撃者にこれらの脆弱性を悪用されることにより、当該製品と連携する GT SoftGOT2000 においてメモリ上の情報が漏えいしたり、GT SoftGOT2000 がサービス停止(DoS)状態に陥る可能性があります。

■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。
また、MELSOFT GT OPC UA Client のバージョンアップに伴い GT SoftGOT2000 も 1.275M 以降の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
MELSOFT GT OPC UA Client	1.03D 以降

【更新手順】

MELSOFT GT OPC UA Client の場合

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 MELSOFT GT OPC UA Client 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. 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。

GT SoftGOT2000 の場合

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。
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。

- ・当該製品をインターネットに接続する場合には、仮想プライベートネットワーク(VPN)等を使用し、成りすましや盗聴を防止してください。
- ・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。
- ・OPC UA サーバを最新版にアップデートしてご使用ください。
- ・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。

■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>