# GENESIS64™ の BACnet®セキュア通信機能における サービス拒否(DoS)及び悪意のあるプログラムが実行される脆弱性

公開日 2023 年 3 月 7 日
最終更新日 2023 年 8 月 30 日
三菱電機株式会社

■概要

GENESIS64™ に搭載している OpenSSL ライブラリにおいて、古典的バッファオーバーフロー(CWE-120)によるサービス拒否(DoS)及び悪意のあるプログラムが実行される脆弱性が存在することが判明しました。当該ライブラリを使用している BACnet®セキュア通信機能が攻撃者により細工された X.509 形式の電子証明書を取り込んだ場合に、サービス停止(DoS)状態に陥ったり(CVE-2022-3602, CVE-2022-3786)、悪意のあるプログラムが実行される(CVE-2022-3602)可能性があります。なお、BACnet®セキュア通信機能はベータ版として製品に搭載されており、初期状態では機能は無効化されています。当該機能を明示的に有効にしない限り当脆弱性の脅威は発生しません。

この脆弱性の影響を受ける GENESIS64™ のバージョンを以下に示しますので、セキュリティパッチを適用してください。

■CVSS スコア

CVE-2022-3602 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H 基本値 8.1
CVE-2022-3786 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H 基本値 5.9

■該当製品の確認方法

<該当製品とバージョン>

GENESIS64™ Version 10.97.2

<バージョンの確認方法>

Windows®のコントロールパネルを開き、「プログラムと機能」を選択します。
名前に「ICONICS Suite」と表示され、バージョンに「10.97.212.46」のバージョン番号が表示されていれば該当します(図 1 参照)。


図 1 Windows®コントロールパネル画面例

■脆弱性の説明

GENESIS64™ に搭載している OpenSSL ライブラリにおいて、X.509 形式の電子証明書に対する検証時の古典的バッファオーバーフロー(CWE-120)による、サービス拒否(DoS)及び悪意のあるプログラムが実行される脆弱性が存在します。

■脆弱性がもたらす脅威

当該ライブラリを使用している BACnet®セキュア通信機能が攻撃者により細工された X.509 形式の電子証明書を取り込むことで、サービス停止(DoS)状態に陥ったり、悪意のあるプログラムが実行される可能性があります。なお、 BACnet®セキュア通信機能はベータ版として製品に搭載されており初期状態では当該機能は無効化されています。当該機能を明示的に有効にしない限り当脆弱性の脅威は発生しません。

■対策方法

GENESIS64™ セキュリティパッチを適用しソフトウェアを更新してください。セキュリティパッチは ICONICS 社運営の Web サイト「ICONICS Community Portal」(https://iconics.force.com/community)の「ダウンロード>アップデート」からダウンロードできます。ダウンロードの際には、同サイト上でアカウントを作成(無料)し、製品に同梱される SupportWorX License Information に記載されている Support WorX Plan Number の入力が必要です。

- 本脆弱性に対するセキュリティパッチ「10.97.2 Critical Fixes Rollup 1」
  (https://iconics.force.com/community/s/software-update/a355a000003g4Q5AAI/10972-critical-fixes-rollup-1)

■軽減策・回避策

上記の対策方法を事情により実施できない場合には、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に、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。

(1) 当該製品の BACnet®セキュア通信機能を有効化している場合は当該機能を無効化します。なお、初期状態では当該機能は無効化されています。当該機能を無効化する手順は GENESIS64 オンラインマニュアル「ICONICS Product Help」(https://docs.iconics.com/V10.97.2/GENESIS64/Help/ICONICS_Product_Help.htm#Com/Intro/ICONICS_Product_Help.htm)の「Home > Common Tools > Data Connectivity > BACnet/SC > Overview of BACnet/SC」にアクセスし、「Using BACnet with the SC Point Manager」の項目をご確認ください。

(2) 制御システムのネットワークとデバイスをファイアウォールで防御し、組織内外を問わず信頼できないネットワークやホストからのアクセスを遮断します。
(3) 制御システムの BACnet®網へのアクセスを物理的に保護し、信頼できないデバイスがシステムに接続されないようにします。

■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

■登録商標
GENESIS64 は、ICONICS,Inc.の商標です。
BACnet は米国暖房冷凍空調学会（ASHRAE）の登録商標です。
Windows は、米国 Microsoft Corporation 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
2023 年 8 月 30 日
古典的バッファオーバーフロー（CWE-120）による悪意のあるプログラムが実行される脆弱性(CVE-2022-3602)の情報を追加し、併せてタイトルを変更しました。