GENESIS64™ の BACnet®セキュア通信機能における OpenSSL に起因する複数の脆弱性

公開日 2023 年 8 月 17 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、複数の脆弱性が存在することが判明しました。これらの脆弱性を悪意のある攻撃者に悪用された場合に、当該製品の情報の漏えいが発生したり、当該製品がサービス停止(DoS)状態に陥ったりする可能性があります(CVE-2022-4203、CVE-2022-4304、CVE-2022-4450、CVE-2023-0401)。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。

これらの脆弱性の影響をうける 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 [1]

CVE-2022-4203	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H	基本値: 4.4
CVE-2022-4304	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N	基本値: 5.9
CVE-2022-4450	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H	基本値: 5.9
CVE-2023-0401	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」から「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™には、以下 4 件の脆弱性が存在します。

CVE-2022-4203	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、具体的には名前制約チェック時の境界外読み取り(CWE-125[2])による、サービス拒否(DoS)の脆弱性が存在します。
CVE-2022-4304	GENESIS64™に搭載している OpenSSL ライブラリにおいて、RSA での復号の実装に存在するタイミングの違いに起因する情報漏えい(CWE-208[3])による情報漏えいの脆弱性が存在します。
CVE-2022-4450	GENESIS64™に搭載している OpenSSL ライブラリにおいて、PEM 形式のデータの読み込み時の二重解放(CWE-415[4])による、サービス拒否(DoS)の脆弱性が存在します。
CVE-2023-0401	GENESIS64™に搭載している OpenSSL ライブラリにおいて、電子署名の検証時の NULL ポインタデリファレンス(CWE-476[5])による、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

これらの脆弱性を悪意のある攻撃者に悪用された場合、当該製品の情報の漏えいが発生したり、当該製品がサービス停止(DoS)状態に陥ったりす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。

CVE-2022-4203	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)状態に陥る可能性があります。
CVE-2022-4304	当該ライブラリを使用している BACnet®セキュア通信機能が、Bleichenbacher 攻撃(パディングエラーが発

1 https://www.ipa.go.jp/security/vuln/CVSSv3.html
2 https://cwe.mitre.org/data/definitions/125.html
3 https://cwe.mitre.org/data/definitions/208.html
4 https://cwe.mitre.org/data/definitions/415.html
5 https://cwe.mitre.org/data/definitions/476.html

生した際の実行時間の違いを観察することにより、暗号文の解読を行う攻撃)を受けることにより、暗号文が解読され、情報が漏えいする可能性があります。

CVE-2022-4450　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 PEM 形式のデータ(公開鍵、電子証明書など)を読み込むことにより、サービス停止(DoS)状態に陥る可能性があります。

CVE-2023-0401　当該ライブラリを使用している BACnet®セキュア通信機能が、FIPS モードを有効にした状態で攻撃者により細工された PKCS7 形式の電子署名を検証することにより、サービス停止(DoS)状態に陥る可能性があります。

■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 2」
  (https://iconicsinc.my.site.com/community/s/software-update/a355a000003g4Q5AAI/10972-critical-fixes-rollup-2)

■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には、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/Apps/WBDT/BACnet_SC/Overview_of_BACnet_SC.htm)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。