GENESIS64™ および MC Works64 における複数の脆弱性

公開日 2024 年 7 月 2 日
三菱電機株式会社

■概要

GENESIS64™ および MC Works64 に、複数の脆弱性が存在することが判明しました。これらの脆弱性が悪意のある攻撃者に悪用された場合、当該製品がサービス停止(DoS)状態に陥ったり、悪意のあるプログラムが実行されたり、適切な認証なしにログインされたりする可能性があります。(CVE-2023-2650、CVE-2023-4807、CVE-2024-1182、CVE-2024-1573、CVE-2024-1574)

これらの脆弱性の影響をうける GENESIS64™ および MC Works64 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または軽減策を適用してください。

■CVSS スコア [1]

CVE-2023-2650 CVSS:v3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L 基本値: 3.7
CVE-2023-4807 CVSS:v3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H 基本値: 5.9
CVE-2024-1182 CVSS:v3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H 基本値: 7.0
CVE-2024-1573 CVSS:v3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N 基本値: 5.9
CVE-2024-1574 CVSS:v3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H 基本値: 6.7

■該当製品の確認方法

<各脆弱性の該当製品とバージョン>

CVE-2023-2650 GENESIS64™ Version 10.97.2
CVE-2023-4807 GENESIS64™ Version 10.97.2
CVE-2024-1182 GENESIS64™ の全てのバージョンおよび MC Works64 の全てのバージョン
CVE-2024-1573 GENESIS64™ Version 10.97 から 10.97.2 および MC Works64 の全てのバージョン
CVE-2024-1574 GENESIS64™ Version 10.97 から 10.97.2 および MC Works64 の全てのバージョン

<バージョンの確認方法>

CVE-2023-2650 および CVE-2023-4807

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。
GENESIS64™ は名前に「ICONICS Suite」と表示され、バージョンに「10.97.212.46」と記載されている場合に該当します。(図 1 参照)。

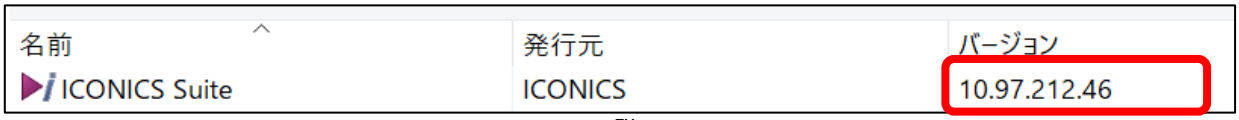

図 1 GENESIS64™ Version 10.97.2

CVE-2024-1182

GENESIS64™ の全てのバージョンおよび MC Works64 の全てのバージョンが該当します。

CVE-2024-1573 および CVE-2024-1574

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。
GENESIS64™ は名前に「ICONICS Suite」と表示され、バージョンに「10.97.212.46」以前のバージョン番号が表示されている場合に該当します(図 1 参照)。
MC Works64 は全てのバージョンが該当します。

■脆弱性の説明

GENESIS64™ および MC Works64 には、以下 5 件の脆弱性が存在します。

CVE-2023-2650 GENESIS64™ の BACnet®セキュア通信機能が有効になっている場合に、当該製品に搭載している OpenSSL ライブラリにおいて、データに対する検証時の制限またはスロットリング無しのリソースの割り当て(CWE-770[2])による、サービス拒否(DoS)の脆弱性が存在します。なお、該当するバージョンに搭載されている BACnet®セキュア通信機能はベータ版であり、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-2023-4807 GENESIS64™ が AVX512-IFMA 命令をサポートする X64_64 CPU 上で動作しており、かつ BACnet®セキュア通信機能が有効になっている場合に、当該製品に搭載している OpenSSL ライブラリにおいて、メッセー

1 https://www.ipa.go.jp/security/vuln/CVSSv3.html
2 https://cwe.mitre.org/data/definitions/770.html

ジ認証コード(MAC)の実装不具合に起因するデジタル署名の不適切な検証（CWE-347[3]）による、サービス拒否(DoS)の脆弱性が存在します。なお、該当するバージョンに搭載されている BACnet®セキュア通信機能はベータ版であり、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-2024-1182 GENESIS64™ および MC Works64 を、マルチエージェント通知機能の Pager エージェントと共にインストールする場合に、ファイル検索パスの制御不備(CWE-427[4])による、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。

CVE-2024-1573 GENESIS64™ および MC Works64 のモバイル監視機能において、下記の条件の全てを満たした環境の場合に、自動ログイン時の不適切な認証(CWE-287[5])による、認証回避の脆弱性が存在します。

- Active Directory を使用する
- 「自動ログイン」オプションを有効にする
- IcoAnyGlass IIS アプリケーションプールを Active Directory ドメインアカウントで実行する
- IcoAnyGlass IIS アプリケーションプールアカウントを GENESIS64 ™ および MC Works64 セキュリティに含め、ログインする権限を与える

CVE-2024-1574 GENESIS64™ および MC Works64 のライセンス機能において、クラスまたはコードを選択する外部から制御された入力の使用（CWE-470[6]）による、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

これらの脆弱性を悪意ある攻撃者に悪用された場合、当該製品がサービス停止(DoS)状態に陥ったり、悪意のあるプログムが実行されたり、適切な認証なしにログインされたりする可能性があります。

CVE-2023-2650 当該ライブラリを使用している BACnet®セキュア通信機能が、攻撃者によって細工された ASN.1 オブジェクト識別子を含む証明書を受信し、検証することで、一時的にサービス停止(DoS)状態に陥る可能性があります。

CVE-2023-4807 当該ライブラリを使用している BACnet®セキュア通信機能が、攻撃者によって細工されたメッセージ認証コード(MAC)を含むメッセージを受信し、処理することで、サービス停止(DoS)状態に陥る可能性があります。

CVE-2024-1182 攻撃者が細工した DLL を特定のフォルダに格納することで、悪意あるプログラムが実行される可能性があります。

CVE-2024-1573 悪意ある第三者が適切な認証を回避してシステムにログインできる可能性があります。

CVE-2024-1574 攻撃者がシステムによって保護されていない特定のファイルを書き換えることで、悪意あるプログラムが管理者権限で実行される可能性があります。

■対策方法

CVE-2023-2650

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 3」
  (https://iconicsinc.my.site.com/community/s/software-update/a355a000003g4Q5AAI/10972-critical-fixes-rollup-3)

CVE-2023-4807

当該バージョンに適用可能なセキュリティパッチを現在開発中で、準備が出来次第、公開予定です。
セキュリティパッチが公開されるまでの間は、下記の軽減策・回避策にてご対応ください。

CVE-2024-1182

本脆弱性に対する対策バージョンのリリース予定はないため、下記の軽減策・回避策にてご対応ください。

CVE-2024-1573 および CVE-2024-1574

GENESIS64™ Version 10.97.3 以降の製品は、この脆弱性の影響を受けません。この脆弱性による脅威を排除するために、GENESIS64™ のアップグレードをご検討ください。

影響を受けるバージョンの GENESIS64™ および MC Works64 を引き続き使用する必要がある場合、三菱電機は以下に記載されている緩和策および回避策を講じることを強く推奨します。

---

3 https://cwe.mitre.org/data/definitions/347.html

4 https://cwe.mitre.org/data/definitions/427.html

5 https://cwe.mitre.org/data/definitions/287.html

6 https://cwe.mitre.org/data/definitions/470.html

■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に、三菱電機は以下に示す軽減策や回避策を講じることを推奨します。

全ての脆弱性

(1) 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。

(2) 当該製品がインストールされた PC および本 PC が接続されているネットワークへの物理的なアクセスを制限し、不正な接触を防止します。

(3) 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ようにします。また信頼できない電子メールの添付ファイルを開かないようにします。

CVE-2023-2650

(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) 信頼できない証明書をインポートしないようにします。

CVE-2023-4807

(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。

CVE-2024-1182

(1) マルチエージェント通知機能は、GENESIS64™ Version 10.97.3 以降ではデフォルトインストールに含まれません。GENESIS64™ Version 10.97.3 以降をインストールする際には、本機能を特に必要としない限り、カスタムインストールしないでください。

CVE-2024-1573

(1) GENESIS64™および MC Works64 のセキュリティ設定にて、下記の 4 つの条件のうち少なくとも 1 つを満たさないように設定してください。

- Active Directory を使用する
- 「自動ログイン」オプションを有効にする
- IcoAnyGlass IIS アプリケーションプールを Active Directory ドメインアカウントで実行する
- IcoAnyGlass IIS アプリケーションプールアカウントを GENESIS64™および MC Works64 セキュリティに含め、ログインする権限を与える

■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。