GENESIS64™ および MC Works64 における複数の脆弱性

公開日 2022 年 7 月 19 日
三菱電機株式会社

■概要

GENESIS64™ および MC Works64 には、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、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、悪意のあるプログラムが実行されたりする可能性があります。(CVE-2022-29834、CVE-2022-33315、CVE-2022-33316、CVE-2022-33317、CVE-2022-33318、CVE-2022-33319、CVE-2022-33320)

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を適用してください。

■CVSS スコア

CVE-2022-29834	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	基本値: 7.5
CVE-2022-33315	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	基本値: 7.8
CVE-2022-33316	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	基本値: 7.8
CVE-2022-33317	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	基本値: 7.8
CVE-2022-33318	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	基本値: 9.8
CVE-2022-33319	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H	基本値: 8.2
CVE-2022-33320	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	基本値: 7.8

■該当製品の確認方法

<該当製品とバージョン>

GENESIS64™ :Version 10.97 から 10.97.1
MC Works64 :Version 4.04E 以前の全てのバージョン (CVE-2022-29834 を除く)

<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。

GENESIS64™ は名前に「ICONICS Suite」と表示され、バージョンに「10.97.112.56」以前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)。

MC Works64 は名前に「MELSOFT MC Works64」と表示され、バージョンに「10.95.210.01」以前のバージョン番号が表示されていれば該当します(図 2 参照)。

図 1 GENESIS64™

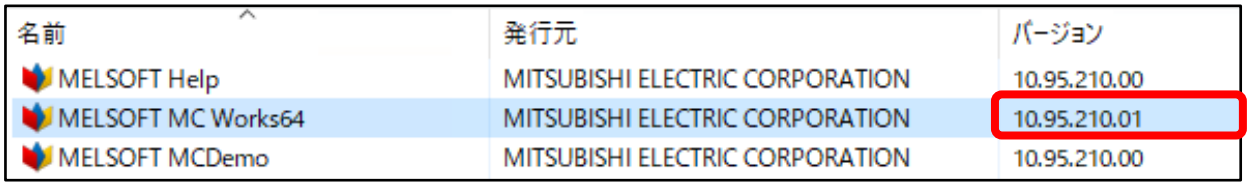

図 2 MC Works64

■脆弱性の説明

GENESIS64™ および MC Works64 に、以下 7 件の脆弱性が存在します。

CVE-2022-29834	GENESIS64™ のモバイル監視機能において、URL パラメータの入力検証の不備を起因としたパス・トラバーサル(CWE-22)による、情報漏えいの脆弱性が存在します。
CVE-2022-33315	GENESIS64™ および MC Works64 のグラフィック画面作成・表示機能において、監視画面ファイルの入力検証の不備を起因とした信頼できないデータのデシリアライゼーション(CWE-502)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-2022-33316	GENESIS64™ および MC Works64 のグラフィック画面作成・表示機能において、監視画面ファイルの入力検証の不備を起因とした信頼できないデータのデシリアライゼーション(CWE-502)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-2022-33317	GENESIS64™ および MC Works64 のグラフィック画面作成・表示機能において、スクリプト機能の制限の不備を起因とした信頼できない制御領域からの機能の組み込み(CWE-829)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-2022-33318	GENESIS64™ および MC Works64 の外部 OPC DA サーバーとの接続機能において、パケットに対する入

力検証の不備を起因とした信頼できないデータのデシリアライゼーション(CWE-502)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-2022-33319　GENESIS64™ および MC Works64 の外部 OPC DA サーバーとの接続機能において、パケットのデータサイズの検証不備を起因とした境界外読み込み（CWE-125）による、情報漏えいおよびサービス停止(DoS)の脆弱性が存在します。

CVE-2022-33320　GENESIS64™ および MC Works64 のプロジェクト管理機能において、プロジェクト構成ファイルの入力検証の不備を起因とした信頼できないデータのデシリアライゼーション(CWE-502)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、悪意のあるプログラムが実行されたりする可能性があります。

CVE-2022-29834　GENESIS64™ のモバイル端末用アプリに配信される監視画面の URL に対し、攻撃者が悪意ある URL パラメータを埋め込み、監視画面へアクセスすることにより、GENESIS64™ サーバーにある任意のファイルに保存された情報が漏えいする可能性があります。

CVE-2022-33315　GENESIS64™ と MC Works64 のグラフィック画面作成・表示機能において、悪意ある XAML コードを含む監視画面ファイルをユーザに読み込ませることにより、悪意のあるプログラムが実行される可能性があります。

CVE-2022-33316　GENESIS64™ と MC Works64 のグラフィック画面作成・表示機能において、悪意ある XAML コードを含む監視画面ファイルをユーザに読み込ませることにより、悪意のあるプログラムが実行される可能性があります。

CVE-2022-33317　GENESIS64™ と MC Works64 のグラフィック画面作成・表示機能において、悪意あるスクリプトを含む監視画面ファイルをユーザに読み込ませることにより、悪意のあるプログラムが実行される可能性があります。

CVE-2022-33318　GENESIS64™ と MC Works64 の外部 OPC DA サーバーとの接続機能において、細工されたパケットを受信すると、悪意のあるプログラムが実行される可能性があります。

CVE-2022-33319　GENESIS64™ と MC Works64 の外部 OPC DA サーバーとの接続機能において、細工されたパケットを受信すると、メモリ上の情報が漏えいしたり、サービス停止(DoS)状態に陥る可能性があります。

CVE-2022-33320　GENESIS64™ および MC Works64 のプロジェクト管理機能において、悪意ある XML コードを含むプロジェクト構成ファイルを読み込ませることにより、悪意のあるプログラムが実行される可能性があります。

■対策方法

GENESIS64™、MC Works64 セキュリティパッチを使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の入手方法を以下に示します。

1. GENESIS64™ セキュリティパッチ

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。

1) GENESIS64™ Version 10.97.1 をご使用の場合

当該バージョンのセキュリティパッチは現在開発中で、2022 年 8 月ごろ公開予定です。下記の軽減策・回避策にてご対応ください。

2) GENESIS64™ Version 10.97 をご使用の場合

当該バージョンのセキュリティパッチは現在開発中で、2022 年 9 月ごろ公開予定です。下記の軽減策・回避策にてご対応ください。

2. MC Works64 セキュリティパッチ

ICONICS Web サイトの「MC Works64 および MC Works32 の脆弱性情報」(https://iconics.com/Support/CERT-MC-Works#jp)からセキュリティパッチをダウンロードしてください。

1) MC Works64 Version 4.04E をご使用の場合

当該バージョンのセキュリティパッチは現在開発中で、2022 年 9 月ごろ公開予定です。下記の軽減策・回避策にてご対応ください。

2) MC Works64 Edge-computing Edition Version 4.04E をご使用の場合

当該バージョンのセキュリティパッチは現在開発中で、2022 年 9 月ごろ公開予定です。下記の軽減策・回避策にてご対応ください。

3) MC Works64 Version 4.00A～4.03D をご使用の場合※1

当社の支社・代理店から MC Works64 Version 4.04E のインストーラを入手していただきインストールした上で、2. 1)のセキュリティパッチを適用してください。

※1 該当製品のバージョンの確認方法において、「MELSOFT MC Works64」のバージョンに「10.95.201.23」以後かつ

「10.95.209.08」以前のバージョン番号が表示される場合が該当します。

4) MC Works64 Version 3.04E 以前をご使用の場合※2
当社の支社・代理店にお問い合わせください。
※2 該当製品のバージョンの確認方法において、「MELSOFT MC Works64」のバージョンに「10.94.178.06」以前のバージョン番号が表示される場合が該当します。

■軽減策・回避策
上記の対策（ソフトウェアの更新）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) 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・外の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) 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。

■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