GENESIS64™ および MC Works64 における複数の脆弱性

公開日 2024 年 11 月 28 日
最終更新日 2025 年 1 月 16 日
三菱電機株式会社

■概要

GENESIS64™ および MC Works64 において、複数の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。攻撃者は、特定のフォルダに細工した DLL を格納したり、細工した DLL に改ざんすることによって、悪意のあるプログラムを実行し、当該製品上の情報を漏えいさせたり、当該製品上の情報を改ざん、破壊、削除したり、当該製品をサービス停止(DoS)状態に陥らせることができる可能性があります(CVE-2024-8299、CVE-2024-8300、CVE-2024-9852)。Dialogic ドライバをインストールせずに Dialogic 社製テレフォニーボードを使用している場合または Dialogic 社製テレフォニーボード以外を使用している場合で、かつ GENESIS64™ および MC Works64 のバージョン 10.97.2 以前の場合には無条件に、バージョン 10.97.3 以降の場合にはマルチエージェント通知機能がインストールされている場合に、CVE-2024-8299 の影響を受けます。また、GENESIS64™ および MC Works64 のバージョン 10.97.2 以前の場合には無条件に、バージョン 10.97.3 以降の場合にはマルチエージェント通知機能がインストールされている場合に、CVE-2024-9852 の影響を受けます。さらに、該当製品がデフォルト以外の、保護されていないフォルダにインストールされている場合に、CVE-2024-8300 の影響を受けます。なお、GENESIS64™ Version 10.97.3 以降の製品では、マルチエージェント通知機能は、デフォルトインストールに含まれません。

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および軽減策・回避策を適用してください。

■CVSS スコア [1]

CVE-2024-8299 CVSS:v3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H 基本値: 7.8
CVE-2024-8300 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-2024-9852 CVSS:v3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H 基本値: 7.8

■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-2024-8299 GENESIS64™ および MC Works64 の全てのバージョン
CVE-2024-8300 GENESIS64™ Version 10.97.2、10.97.2 CFR1、10.97.2 CFR2、10.97.3
CVE-2024-9852 GENESIS64™ および MC Works64 の全てのバージョン

<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。

【MC Works64 を使用している場合】

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記載されている場合に該当します(図 1 参照)。

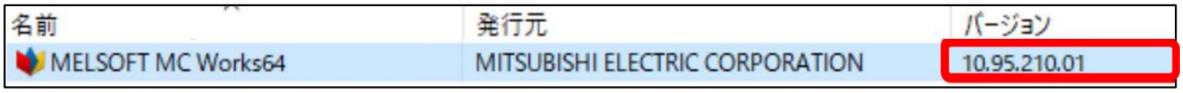

図 1 MC Works64 Version 4.04E(10.95.2)

【GENESIS64™ Version 10.97.2 を使用している場合】

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記載されている場合に該当します(図 2 参照)。

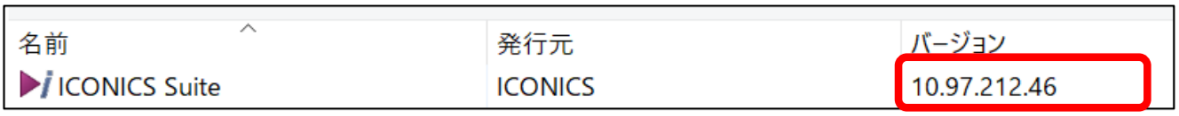

図 2 GENESIS64™ Version 10.97.2

Critical Fixes Rollup(CFR)を適用している場合には、Windows®の設定メニューを開き、アプリ>インストールされているアプリから CFR のバージョンをご確認ください。

【GEENSIS64™ Version 10.97.3 を使用している場合】

GENESIS64™ は名前に「ICONICS Suite」と表示され、バージョンに「10.97.306.55」と記載されている場合に該当します(図 3 参照)。

図 3 GENESIS64™ Version 10.97.3

[1] https://www.ipa.go.jp/security/vuln/CVSSv3.html

■脆弱性の説明

GENESIS64™および MC Works64 には、以下の 3 件の脆弱性が存在します。

CVE-2024-8299　GENESIS64 ™および MC Works64 のマルチエージェント通知機能の Phone エージェントにおいて、ファイル検索パスの制御不備(CWE-427[2])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。Dialogic ドライバをインストールせずに Dialogic 社製テレフォニーボードを使用している場合または Dialogic 社製テレフォニーボード以外を使用している場合で、かつ GENESIS64 ™および MC Works64 のバージョン 10.97.2 以前の場合には無条件に、バージョン 10.97.3 以降の場合にはマルチエージェント通知機能がインストールされている場合に、本脆弱性の影響を受けます。

CVE-2024-8300　GENESIS64™ の FA 機器通信ドライバにおいて、デッドコード(CWE-561[3])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。該当製品がデフォルト以外の、保護されていないフォルダにインストールされている場合に、本脆弱性の影響を受けます。

CVE-2024-9852　GENESIS64™ および MC Works64 のマルチエージェント通知機能の Fax エージェントにおいて、ファイル検索パスの制御不備(CWE-427)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。GENESIS64™ および MC Works64 のバージョンが、10.97.2 以前の場合には無条件に、10.97.3 以降の場合にはマルチエージェント通知機能がインストールされている場合に、本脆弱性の影響を受けます。

■脆弱性がもたらす脅威

攻撃者は、特定のフォルダに細工した DLL を格納したり、細工した DLL を改ざんすることによって、悪意のあるプログラムを実行し、当該製品上の情報を漏えいさせたり、当該製品上の情報を改ざん、破壊、削除したり、当該製品をサービス停止(DoS)状態に陥らせることができる可能性があります。

CVE-2024-8299　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、悪意のあるプログラムを実行し、当該製品上の情報を漏えいさせたり、当該製品上の情報を改ざん、破壊、削除したり、当該製品をサービス停止(DoS)状態に陥らせる可能性があります。

CVE-2024-8300　攻撃者が、細工した DLL に改ざんすることで、悪意のあるプログラムを実行し、当該製品上の情報を漏えいさせたり、当該製品上の情報を改ざん、破壊、削除したり、当該製品をサービス停止(DoS)状態に陥らせる可能性があります。

CVE-2024-9852　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、悪意のあるプログラムを実行し、当該製品上の情報を漏えいさせたり、当該製品上の情報を改ざん、破壊、削除したり、当該製品をサービス停止(DoS)状態に陥らせる可能性があります。

■お客様での対応

CVE-2024-8299

Phone エージェントを使用する必要があり、Dialogic 社製テレフォニーボードを使用している場合には、Dialogic 社から提供されたドライバをインストールしてください。

Phone エージェントを使用する必要があり、Dialogic 社製テレフォニーボード以外を使用している場合には、対策版のリリース予定はございませんので、下記の軽減策・回避策を実施してください。

CVE-2024-8300

「■製品での対応」に記載されているセキュリティパッチを適用してください。

CVE-2024-9852

対策版のリリース予定はございませんので、下記の軽減策・回避策を実施してください。

■製品での対応

CVE-2024-8299

本脆弱性に対する対策版のリリース予定はございません。

CVE-2024-8300

各バージョンに対応するセキュリティパッチは以下のとおりです。

【GENESIS64™ Version 10.97.2 系を使用している場合】

●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)

【GENESIS64™ Version 10.97.3 系を使用している場合】

●本脆弱性に対するセキュリティパッチ「10.97.3 Critical Fixes Rollup 1」
(https://iconicsinc.my.site.com/community/s/software-update/a35QQ000000y2oXYAQ/10973-critical-fixes-rollup-1)

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

3 https://cwe.mitre.org/data/definitions/561.html

CVE-2024-9852
本脆弱性に対する対策版のリリース予定はございません。

■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) 該当製品がインストールされた PC を LAN 内で使用し、信頼できないネットワークやホスト、ユーザからのリモートログインをブロックします。
(2) 該当製品がインストールされた PC をインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク(VPN)等で不正アクセスを防止したうえで、信頼できるユーザのみにリモートログインを許可します。
(3) 該当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。
(4) 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-2024-8299
マルチエージェント通知機能を使用する必要がない場合には、マルチエージェント通知機能をアンインストールしてください。なお、GENESIS64 ™ Version 10.97.3 以降の製品では、マルチエージェント通知機能は、デフォルトインストールに含まれません。
マルチエージェント通知機能を使用する必要があり、かつ Phone エージェントが不要な場合には、マルチエージェント通知機能のカスタムインストールを実行し、Phone エージェントをインストールの対象から除外してください。

CVE-2024-8300
該当製品をデフォルト以外の保護されていないフォルダにインストールしないでください。

CVE-2024-9852
マルチエージェント通知機能を使用する必要がない場合には、マルチエージェント通知機能をアンインストールしてください。なお、GENESIS64 ™ Version 10.97.3 以降の製品では、マルチエージェント通知機能は、デフォルトインストールに含まれません。
マルチエージェント通知機能を使用する必要があり、かつ Fax エージェントが不要な場合には、マルチエージェント通知機能のカスタムインストールを実行し、Fax エージェントをインストールの対象から除外してください。
Fax エージェントをインストールする場合には、Windows®の「Windows FAX とスキャン」を有効にしてください。「Windows FAX とスキャン」を有効にする手順は、Windows®のバージョンによって異なりますので、Microsoft のサイト等で詳細をご確認ください。Window®11 の場合の例を以下に示します。

(1)Windows®11 の「設定」を開きます。
(2)「システム」の「オプション機能」をクリックします。
(3)「オプション機能を追加する」の「機能を表示」をクリックします。
(4)「オプションを追加する」ウィンドウを下へスクロールし、「Windows FAX とスキャン」にチェックボックスを入れて、「次へ」をクリックします。
(5)「追加」をクリックして、インストールを実行します。
(6)インストールが完了したら、PC を再起動します。

■謝辞
これらの脆弱性をご報告いただいた、Palo Alto Networks 社のセキュリティ研究者である Asher Davila 氏と Malav Vyas 氏に感謝いたします。

■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。
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
2025 年 1 月 16 日
「概要」、「脆弱性の説明」及び「軽減策・回避策」を更新しました。