GENESIS64™ および MC Works64 における
情報の漏えい、改ざんおよびサービス拒否(DoS)の脆弱性

公開日 2024 年 10 月 22 日
三菱電機株式会社

■概要

GENESIS64™ および MC Works64 のインストーラに同梱されている GenBroker32 において、GENESIS64™ または MC Works64 と同一の PC にインストールされている場合に、インストール時のフォルダへの不適切な権限の設定に起因する情報の漏えい、改ざんおよびサービス拒否(DoS)の脆弱性が存在することが判明しました。攻撃者は、不適切な権限が設定されたフォルダへアクセスすることによって、当該フォルダに保存されている機密情報やデータを窃取又は改ざんしたり、システムをサービス停止(DoS)状態に陥らせることができる可能性があります。(CVE-2024-7587)

この脆弱性の影響をうける GenBroker32 インストーラが同梱されている 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-2024-7587 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

<該当製品とバージョン>

GENESIS64™ Version 10.97.3 以前の全てのバージョン
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。
GENESIS64™ は名前に「ICONICS Suite」と表示され、バージョンに「10.97.306.55」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 GENESIS64™ Version 10.97.3

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 2 参照)。

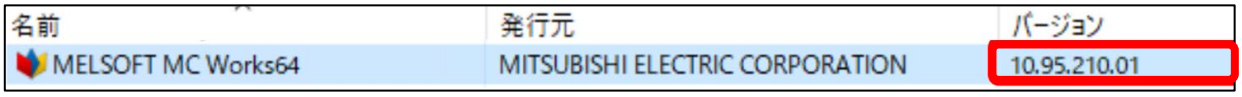

図 2 MC Works64 Version 4.04E

■脆弱性の説明

該当製品のインストーラに同梱されている GenBroker32 が、GENESIS64™ または MC Works64 と同一の PC にインストールされている場合に、不適切なデフォルトパーミッション(CWE-276[2])による、情報の漏えい、改ざんおよびサービス拒否(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ある攻撃者に悪用された場合に、C:¥ProgramData¥ICONICS へアクセスされることによって、当該フォルダに保存されている機密情報やデータが漏えいしたり、改ざんされたり、システムがサービス停止(DoS)状態に陥る可能性があります。

■対策方法

<GENESIS64™ Version 10.97.3 をご使用のお客様>

GenBroker32 をアンインストールした上で、GENESIS64™ にセキュリティパッチを適用し、GenBroker32 を再インストールしてください。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。

1 https://www.ipa.go.jp/security/vuln/CVSSv3.html
2 https://cwe.mitre.org/data/definitions/276.html

〈GENESIS64™ Version 10.97.2 以前（MC Works64 を含む）をご使用のお客様〉
GENESIS64™ Version 10.97.3 に製品をアップグレード頂き、上記の手順に従って GenBroker32 を再インストールしてください。製品のアップグレードが難しい場合には、回避策および軽減策を適用してください。

■回避策
GenBroker32 をインストールした PC の C:¥ProgramData¥ICONICS 及びその配下にある全てのフォルダの権限から”Everyone”を手動で削除してください。配下にあるフォルダも含めて、一括で権限を削除する場合は以下の手順を実施してください。

(1) PC の C:¥ProgramData¥ICONICS のフォルダを右クリックしてプロパティ画面を開く
(2) セキュリティタブを開く
(3) 詳細設定をクリックする
(4) アクセス許可の変更をクリックする
(5) “Everyone”を選択して、「子オブジェクトのアクセス許可エントリすべてを、このオブジェクトから継承可能なアクセス許可エントリで置き換える」のチェックボックスにチェックを入れる
(6) 削除をクリックする

■軽減策
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を講じることを推奨します。

(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する。
(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する。
(3) 当該製品がインストールされた PC、および同 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) 該当製品を使用する PC にウイルス対策ソフトをインストールしたうえで、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たり、信頼できない電子メールの添付ファイルを開いたりしないようにします。

■謝辞
こ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