

GENESIS64 および MC Works64 における情報漏えいの脆弱性

公開日 2022 年 1 月 20 日
三菱電機株式会社

■概要

GENESIS64 および MC Works64 において、認証情報の平文保存(CWE-256)による情報漏えいの脆弱性が存在することが判明しました。当該製品の機能の一つである GridWorX(データベース連携機能)の設定情報を CSV ファイルへ出力すると、認証情報が平文で CSV ファイルに保存され、当該 CSV ファイルを入手したローカルアクセス可能な攻撃者により、データベースへ不正にアクセスされる可能性があります。(CVE-2022-23129)

この脆弱性の影響を受ける 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-2022-23129 CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:H 基本値:7.7

■該当製品の確認方法

<該当製品とバージョン>

GENESIS64 :Version 10.97

MC Works64 :Version 4.04E 以前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「10.97.020.27」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)。

名前	発行元	バージョン
ICONICS LanguagePack for 10.97	ICONICS	10.97.020.27
ICONICS Suite	ICONICS	10.97.020.27

図 1 GENESIS64

名前	発行元	バージョン
MELSOFT Help	MITSUBISHI ELECTRIC CORPORATION	10.95.210.00
MELSOFT MC Works64	MITSUBISHI ELECTRIC CORPORATION	10.95.210.01
MELSOFT MCDemo	MITSUBISHI ELECTRIC CORPORATION	10.95.210.00

図 2 MC Works64

■脆弱性の説明

GENESIS64 および MC Works64 において、認証情報の平文保存(CWE-256)による情報漏えいの脆弱性が存在します。

■脆弱性がもたらす脅威

当該製品の機能の一つである GridWorX(データベース連携機能)の設定情報を CSV ファイルへ出力すると、認証情報が平文で CSV ファイルに保存され、当該 CSV ファイルを入手したローカルアクセス可能な攻撃者により、データベースへ不正にアクセスされる可能性があります。(CVE-2022-23129)

■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 の割り付けが必要です。

1) GENESIS64 Version 10.97 をご使用の場合

「10.97 Critical Fixes Rollup 2」

(<https://iconics.force.com/community/s/software-update/a355a00000304zLAAS/1097-critical-fixes-rollup-2-including-language-pack-and-devicexplorer-640>)

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
「MC Works64 Version 4.04E (Version 10.95.210.01) セキュリティパッチ」
- 2) MC Works64 Edge-computing Edition Version 4.04E をご使用の場合
「MC Works64 Version 4.04E (Version 10.95.210.01) セキュリティパッチ」
- 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 をご使用の場合
「MC Works64 Version 3.04E (Version 10.94.178.06) セキュリティパッチ」
- 5) MC Works64 Version 3.00A～3.03D をご使用の場合 ^{※2}
当社の支社・代理店から MC Works64 Version 3.04E 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. 4)のセキュリティパッチを適用してください。

※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「10.92.173.77」以後かつ「10.94.177.23」以前のバージョン番号が表示される場合が該当します。

- 6) MC Works64 Version 2.02C 以前をご使用の場合 ^{※3}
当社の支社・代理店にお問い合わせください。

※3 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「10.87.148.42」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(セキュリティパッチの適用)を事情により実施できない場合、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、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) GridWorX の設定情報を CSV ファイルへ出力した後、CSV ファイル中に記載されている SQL データベースの認証情報(パスワード)を削除します。
- (2) GridWorX の設定情報を CSV ファイルへ出力する前に、SQL データベースの認証情報(パスワード)を削除します。
- (3) GridWorX の設定情報を CSV ファイルへ出力する権限を管理者以外のユーザに付与しないよう、セキュリティ機能の設定を変更します。
- (4) 制御システムネットワークとリモートデバイスをファイアウォールで防御し、ビジネスネットワークから分離します。
- (5) すべての制御システムデバイスやシステムのネットワークへの接続を最小限に抑え、信頼できるネットワークやホストからのみアクセスできるようにします。

■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>