

GENESIS64 および MC Works64 のデータベースサーバーにおけるサービス拒否 (DoS) 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 のデータベースサーバーにおいて、バッファオーバーリード(CWE-126)によるサービス拒否 (DoS) の脆弱性が存在することが判明しました。正規のユーザーが、攻撃者によって細工されたスタアドプロシージャを含む設定ファイルを、当該製品へインポートし、当該製品からデータベースに対してコマンドを実行することにより、データベースサーバーがサービス拒否(DoS)状態に陥る可能性があります。(CVE-2022-23130)

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-2022-23130 CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:C/C:N/I:L/A:H 基本値: 5.9

■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 4.00A から 4.04E

〈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「10.95.201.23」から「10.95.210.01」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 のデータベースサーバーにおいて、バッファオーバーリード(CWE-126)によるサービス拒否 (DoS) の脆弱性が存在します。

■脆弱性がもたらす脅威

正規のユーザーが細工されたスタアドプロシージャを含む設定ファイルを GENESIS64 又は MC Works64 へインポートし、データベースに対してコマンドを実行することにより、GENESIS64 および MC Works64 のデータベースサーバーがサービス拒否(DoS)状態に陥る可能性があります。(CVE-2022-23130)

■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/a355a000003O4zLAAS/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 ※
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。

※ 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。

■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) 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。
- (2) 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。
- (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。

■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>