

# GENESIS64 および MC Works64 の AutoCAD(DWG)ファイルのインポート機能における情報漏えいと悪意あるプログラムが実行される脆弱性

公開日 2021 年 10 月 21 日  
最終更新日 2021 年 11 月 25 日  
三菱電機株式会社

## ■概要

GENESIS64 および MC Works64 の AutoCAD(DWG)ファイルのインポート機能において、境界外読み取り(CWE-125)による情報漏えいの脆弱性、及び境界外書き込み(CWE-787)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することが判明しました。攻撃者により細工された AutoCAD(DWG)ファイルを当該製品にインポートすることで、情報漏えいや、悪意のあるプログラムの実行が発生する可能性があります。(CVE-2021-27040、CVE-2021-27041)

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-2021-27040 CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N 基本値:3.3

CVE-2021-27041 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

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 と MC Works64 の AutoCAD(DWG)ファイルインポート機能において、境界外読み取り(CWE-125)による情報漏えいの脆弱性(CVE-2021-27040)、及び境界外書き込み(CWE-787)による悪意のあるプログラムが実行される脆弱性(CVE-2021-27041)が存在します。

## ■脆弱性がもたらす脅威

GENESIS64 と MC Works64 には、細工された AutoCAD(DWG)ファイルをインポートすると、情報漏えいや悪意のあるプログラムの実行が発生す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 Web サイトの「SECURITY UPDATES」(<https://iconics.com/Support/CERT>)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) GENESIS64 Version 10.97 をご使用の場合

「10.97 Critical Fixes Rollup 2」

## 2. MC Works64 セキュリティパッチ

ICONICS Web サイトの「MC Works64 AND MC Works32 SECURITY UPDATES / MC Works64 および MC Works32 の脆弱性情報」(<https://iconics.com/Support/CERT-MC-Works>)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。
- 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  
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。
- 6) MC Works64 Version 2.02C 以前をご使用の場合※  
当社の支社・代理店にお問い合わせください。

※ 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「10.87.148.42」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) 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>

### ■更新履歴

2021年11月25日

境界外読み取り(CWE-125)による情報漏えいの脆弱性(CVE-2021-27040)の情報を追加