GENESIS64、ICONICS Suite、MobileHMI及びMC Works64の ソフトウェアキーボード機能における 悪意のあるプログラムが実行される脆弱性

公開日 2025年12月18 日
三菱電機株式会社

■概要

GENESIS64、ICONICS Suite、MobileHMI及びMC Works64のソフトウェアキーボード機能（以下「キーパッド機能」）において、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、キーパッド機能の設定ファイルを改ざんすることにより、正規ユーザがキーパッド機能を利用した際に、任意の実行ファイル（EXE）を実行させることができます（CVE-2025-11774）。これにより、攻撃者は実行されたEXEを介して、該当製品がインストールされたPCに保存されている情報を窃取若しくは改ざん又は削除・破壊をしたり、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。

本脆弱性の影響を受ける製品及びバージョンを以下に示しますので、「■お客様での対応」に記載されている対応を実施してください。

■CVSSスコア[1]

CVE-2025-11774　CVSS:v3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H 基本値: 8.2

■該当製品の確認方法

<各脆弱性の該当製品とバージョン>
GENESIS64： Version 10.97.2 CFR3以前の全てのバージョン
ICONICS Suite: Version 10.97.2 CFR3以前の全てのバージョン
MobileHMI: Version 10.97.2 CFR3以前の全てのバージョン
MC Works64： 全てのバージョン

<バージョン確認方法>
Windowsのコントロールパネルを開き、「プログラム」の「プログラムと機能」を選択します。
名前に「GENESIS64」、「ICONICS Suite」または「MobileHMI」と表示され、バージョンが「10.97.212.46」以下である場合に該当します。（図 1）

図1 該当製品とバージョン表示

■脆弱性の説明

GENESIS64、ICONICS Suite、MobileHMI及びMC Works64のキーパッド機能において、OSコマンドインジェクション(CWE-78[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。

■脆弱性がもたらす脅威

攻撃者は、キーパッド機能の設定ファイルを改ざんすることにより、正規ユーザがキーパッド機能を利用した際に、任意のEXEを実行させることができます。これにより、攻撃者は実行されたEXEを介して、該当製品がインストールされたPCに保存されている情報を窃取若しくは改ざん又は削除・破壊をしたり、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。

■お客様での対応

<MC Works64を使用中のお客様>
セキュリティパッチ及び対策版のリリース予定はございません。
本脆弱性が悪用されるリスクを最小限に抑えるため、GENESIS64 Version 10.97.3 以降への置き換えをご検討ください。
GENESIS64 への置き換え方法については、以下のドキュメントをご参照ください。

「GENESIS64 – How to replace MC Works64 with GENESIS64_JP」
(https://www.mitsubishielectric.co.jp/dl/fa/members/document/manual/scada/bcn-p5999-1459/bcnp59991459a.pdf)

<GENESIS64、ICONICS Suite又はMobileHMIを使用中のお客様>
本脆弱性は、GENESIS64 Version 10.97.3で修正されています。
GENESIS64 Version 10.97.3へアップデートを実施した後に、最新のパッチバージョンを適用してください。または、最新製品で

[1] https://www.ipa.go.jp/security/vuln/CVSSv3.html
[2] https://cwe.mitre.org/data/definitions/78.html

あるGENESIS V11へのバージョンアップを実施してください。Version 10.97.3及び最新のパッチバージョンの入手先は、「■製品での対応」を参照してください。

■製品での対応

〈MC Works64〉

対策版のリリース予定はございません。

〈GENESIS64、ICONICS Suite又はMobileHMI〉

Version 10.97.3は、MEIDS社のポータルサイト(https://iconicsinc.my.site.com/community)にアクセスし、「Resources > Product Downloads > 10.97.3」からダウンロードいただけます。

最新のVersion 10.97.3向けパッチバージョンは、下記からダウンロードいただけます。
https://iconicsinc.my.site.com/community/s/software-update/a35QQ000000y2oXYAQ/10973-critical-fixes-rollup-2

■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、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からのリモートログインをブロックしてください。
(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てください。
(3) 該当製品がインストールされたPC及び本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てください。
(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てください。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てください。
(5) 該当製品がインストールされたPCに、ウィルス対策ソフトを搭載してください。

■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