GENESIS64、MC Works64 及び GENESIS の
複数のプロセスにおける情報改ざんの脆弱性

公開日 2025 年 8 月 5 日
三菱電機株式会社

■概要

GENESIS64、MC Works64 及び GENESIS の複数のプロセスにおいて、情報改ざんの脆弱性が存在することが判明しました。攻撃者は、該当製品のプロセスが書き込み先として使用するファイルから攻撃対象のファイルへのシンボリックリンクを作成し、正規のユーザに同プロセスを実行させることで、任意のファイルへの不正な書き込みを行わせることができます(CVE-2025-7376)。これにより、攻撃者は、該当製品がインストールされた PC 上のファイルを破壊できる可能性があり、結果として PC 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。

本脆弱性の影響をうける GENESIS64、MC Works64 及び GENESIS の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-2025-7376　CVSS:v3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:N/I:H/A:N　基本値: 5.9

■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 及び MC Works64： 全てのバージョン
GENESIS： Version 11.00

<GENESIS のバージョン確認方法(Windows 11)>

Windows の設定を開き、「アプリ」>「インストールされたアプリ」を選択します。
「ICONICS GENESIS」のバージョンに「11.0.812」と表示されていれば該当します(図 1 参照)。

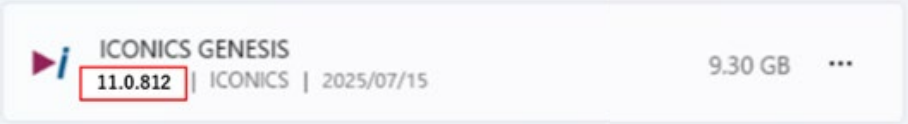

図1 GENESIS Version 11.00

■脆弱性の説明

GENESIS64、MC Works64 及び GENESIS の複数のプロセスにおいて、Windows ショートカットのフォロー(CWE-64[2])による、情報改ざんの脆弱性が存在します。

■脆弱性がもたらす脅威

攻撃者は、該当製品のプロセスが書き込み先として使用するファイルから攻撃対象のファイルへのシンボリックリンクを作成し、正規のユーザに同プロセスを実行させることで、任意のファイルへの不正な書き込みを行わせることができます。これにより、攻撃者は、該当製品がインストールされた PC 上のファイルを、破壊できる可能性があります。破壊されたファイルが当該 PC の動作に必要なファイルの場合には、当該 PC がサービス停止(DoS)状態に陥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>
対策版のリリース予定はございませんので、下記の軽減策にて対応をお願いいたします。

<GENESIS64 を使用中のお客様>
本脆弱性に対する対策を含むバージョンを現在開発中で、準備ができ次第、公開予定です。
公開されるまでの間は、下記の軽減策にて対応をお願いいたします。

<GENESIS を使用中のお客様>
「■製品での対応」に記載されている最新の GENESIS をダウンロードし、適用してください。

■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。

---

1 https://www.ipa.go.jp/security/vuln/CVSSv3.html
2 https://cwe.mitre.org/data/definitions/64.html

〈GENESIS64〉
本脆弱性に対する対策を含むバージョンを現在開発中です。

〈GENESIS〉
本脆弱性に対する対策を含むバージョンは以下のとおりです。
●GENESIS Version 11.01 以降の最新版
下記からダウンロードいただけます。
https://iconicsinc.my.site.com/community/s/resource-center/product-downloads

■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 に管理者以外がログインできないように設定してください。
(2) 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、管理者以外のユーザからのリモートログインをブロックします。
(3) 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、管理者のみにリモートログインを許可します。
(4) 該当製品がインストールされた PC および本 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ます。
(5) 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