GENESIS64 および MC Works64 の Web 通信機能における認証回避の脆弱性

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 Web 通信機能において、不完全なブラックリスト(CWE-184)による認証回避の脆弱性が存在することが判明しました。攻撃者は当該製品の機能の一つである FrameWorX サーバーに対して、細工した WebSocket プロトコルのパケットを送信することで、GENESIS64 および MC Works64 の認証を回避し、当該製品を不正に操作できる可能性があります。(CVE-2022-23128)

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-2022-23128　CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H　基本値:9.8

■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 4.00A 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)。

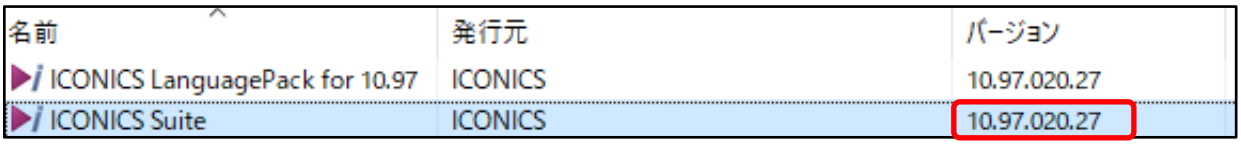

図 1　GENESIS64

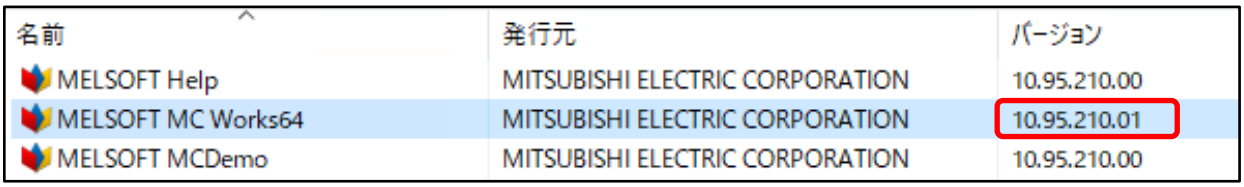

図 2　MC Works64

■脆弱性の説明

GENESIS64 および MC Works64 の Web 通信機能において、不完全なブラックリスト(CWE-184)による認証回避の脆弱性が存在します。

■脆弱性がもたらす脅威

攻撃者は当該製品の機能の一つである FrameWorX サーバに対して、細工した WebSocket プロトコルのパケットを送信することで、GENESIS64 又は MC Works64 の認証を回避し、当該製品を不正に操作できる可能性があります。(CVE-2022-23128)

■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) FrameWorX サーバーの通信方式を WebSocket 通信から WCF 通信に切り替えます。当該製品のインストール先フォルダにある「FwxServer.Network.config」ファイルの「WebSocketsTransport」項目を「false」に編集してください。
(2) 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。
(3) 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