GENESIS64 および MC Works64 の OPC UA 通信機能における サービス拒否(DoS)の脆弱性

公開日 2021 年 10 月 21 日
三菱電機株式会社

■概要

GENESIS64 および MC Works64 において、製品に搭載している OPC UA SDK にサービス拒否(DoS)の脆弱性が存在することが判明しました。攻撃者により細工されたパケットを受信することで、当該製品がサービス停止状態に陥る可能性があります(CVE-2021-27432)。

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-2021-27432 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H 基本値:7.5

■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)。

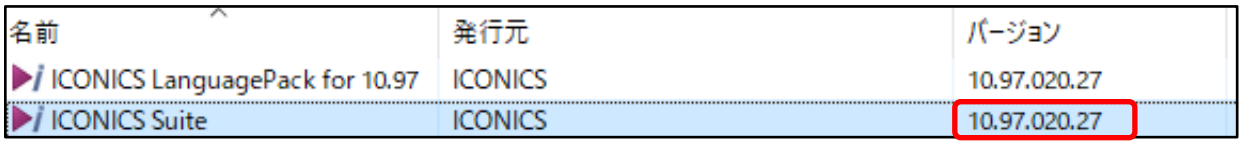

図 1 GENESIS64

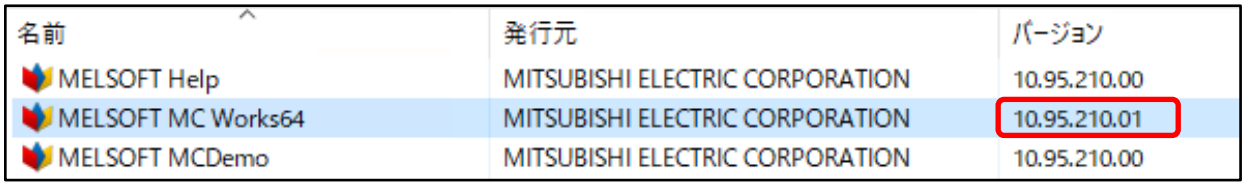

図 2 MC Works64

■脆弱性の説明

GENESIS64 と MC Works64 の OPC UA 通信機能において、不適切な再帰制御(CWE-674)によるサービス拒否(DoS)の脆弱性(CVE-2021-27432)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 OPC UA の通信パケットを受信すると、サービス拒否(DoS)状態に陥る可能性があります。

■対策方法

GENESIS64、MC Works64 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) GENESIS64 および MC Works64 が信頼できる OPC UA サーバ、クライアントとのみ接続するよう、OPC UA のセキュリティ証明書を利用します。

■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