MC Works64 のモバイル監視における情報漏えいの脆弱性

公開日 2022 年 1 月 20 日
三菱電機株式会社

■概要

MC Works64 のモバイル監視において、入力検証の不備を起因とした反射型クロスサイトスクリプティング（CWE-79）による情報漏えいの脆弱性が存在することが判明しました。攻撃者は、MC Works64 サーバーからモバイル端末用アプリ(MC Mobile)に配信される監視画面への URL に悪意のあるスクリプトを埋め込み、ユーザに本 URL へアクセスさせることによって、MC Works64 サーバーの認証情報を窃取することができます。攻撃者は、窃取した認証情報を用いて、任意の操作を行うことができます。（CVE-2022-23127）

この脆弱性の影響を受ける 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-2022-23127　CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N　基本値：4.2

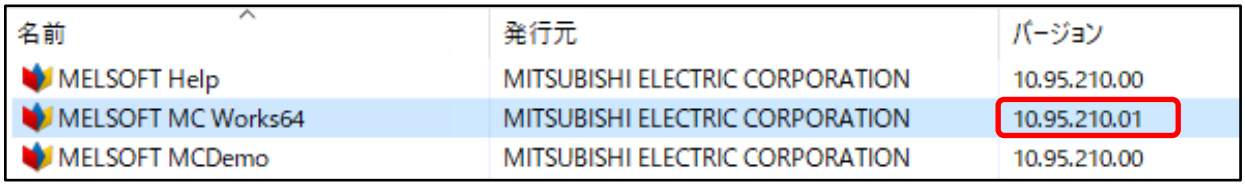
■該当製品の確認方法

〈該当製品とバージョン〉

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。
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 1 参照)。



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 1　MC Works64

■脆弱性の説明

MC Works64 のモバイル監視において、入力検証の不備を起因とした反射型クロスサイトスクリプティング（CWE-79）による情報漏えいの脆弱性が存在します。

■脆弱性がもたらす脅威

攻撃者は、MC Works64 サーバーからモバイル端末用アプリ(MC Mobile)に配信される監視画面への URL に悪意のあるスクリプトを埋め込み、ユーザに本 URL へアクセスさせることによって、MC Works64 サーバーの認証情報を窃取することができます。攻撃者は、窃取した認証情報を用いて、任意の操作を行うことができます。（CVE-2022-23127）

■対策方法

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。

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※1
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、1)のセキュリティパッチを適用してください。

※1 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。

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※2
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、4)のセキ

ュリティパッチを適用してください。

※2 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「10.92.173.77」以後かつ「10.94.177.23」以前のバージョン番号が表示される場合が該当します。

6) MC Works64 Version 2.02C 以前をご使用の場合※3
当社の支社・代理店にお問い合わせください。

※3 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