MC Works64 および MC Works32 のサービス拒否とリモートから任意のコードが実行される脆弱性

公開日 2020 年 6 月 18 日
最終更新日 2021 年 6 月 14 日
三菱電機株式会社

■概要

MC Works64 および MC Works32 には、複数の脆弱性が存在することが判明しました。攻撃者は、細工したデータを送信することにより、対象をサービス拒否(DoS)状態に陥らせることや、任意のコードを実行することができます。

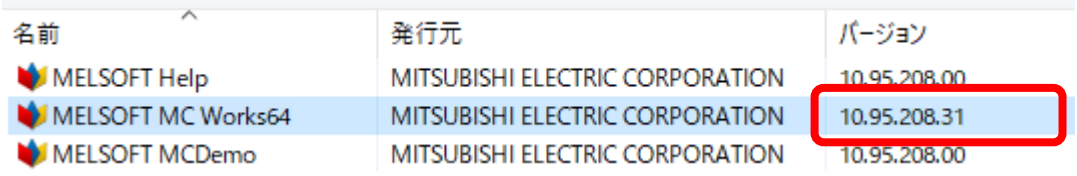
この問題の影響をうける MC Works64 および MC Works32 のバージョンを以下に示しますので、セキュリティパッチを適用してください。

■該当製品の確認方法

<該当製品とバージョン>

MC Works64 ：Version 4.02C (Version 10.95.208.31)*1 以前の全てのバージョン
MC Works32 ：Version 3.00A (Version 9.50.255.02)*1

*1 [コントロールパネル]－[プログラムと機能]に表示される MC Works64 と MC Works32 のバージョン
Windows®スタートメニューから、[Windows システムツール]→[コントロールパネル]→[プログラムと機能]を選択します。
MC Works64 は「MELSOFT MC Works64」、MC Works32 は「Mitsubishi Electric MC Works」と表示されます。



<バージョン情報>

■脆弱性の説明

MC Works64 および MC Works32 に、以下 5 件の脆弱性が存在します。

①MC Works64 の MC Broker64 または MC Works32 の MC Broker32 は、細工されたパケットを受信すると、領域外へのメモリアクセスにより、サービス拒否(DoS)状態に陥るか、リモートから任意のコードが実行される可能性があります。(CWE-787)

②MC Works64 のプラットフォームサービスは、細工されたパケットを受信すると、データ復元処理の不備により、サービス拒否(DoS)状態に陥る可能性があります。(CWE-502)

③MC Works64 Workbench の Pack&Go 機能は、細工されたパッケージファイルを受信すると、データ復元処理の不備により、リモートから任意のコードが実行される可能性があります。(CWE-502)

④MC Works64 の GridWorX サーバは、カスタムクライアント機能からの細工されたメッセージを受信することにより、内部データの漏えいや改ざんの可能性、およびリモートから任意の SQL 文が実行される可能性があります。(CWE-94)

⑤MC Works64 の FrameWorX サーバは、細工されたパケットを受信すると、データ復元処理の不備により、サービス拒否(DoS)状態に陥るか、リモートから任意のコードが実行される可能性があります。(CWE-502)

■脆弱性がもたらす脅威

これらの脆弱性が悪用された場合、リモートからコードが実行されたり、サービス拒否(DoS)状態に陥ったり、情報の漏えいや改ざんが発生する可能性があります。

■対策方法

セキュリティパッチを「MC Works64 および MC Works32 の脆弱性情報」の Web ページからダウンロードし、ソフトウェアを更新してください。この Web ページは当社グループ会社の ICONICS にて運営されています。

<MC Works64 Version 4.00A～4.02C 向けセキュリティパッチ>

MC Works64 Version 4.00A (Version 10.95.201.23)
MC Works64 Version 4.02C (Version 10.95.208.31)
MC Works64 Edge-computing Edition Version 4.00A (Version 10.95.201.37) ※
MC Works64 Edge-computing Edition Version 4.01B (Version 10.95.201.40) ※
MC Works64 Edge-computing Edition Version 4.02C (Version 10.95.208.31)
※ Version 4.00A と 4.01B のセキュリティパッチは、同一の"MC_Works64_Edge_computing_Edition_Version_4_00A_01B_(Version_10_95_201_37)_Security_Patches.zip"です。

<MC Works64 Version 3.00A～3.04E 向けセキュリティパッチ>

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く必要があります。Version 3.04E をインストールした上で、下記のセキュリティパッチを適用してください。
MC Works64 Version 3.04E (Version 10.94.178.06)

<MC Works64 Version 2.00A～2.02C 向けセキュリティパッチ>

当社の支社・代理店から MC Works64 Version 2.02C のインストーラを入手していただく必要があります。Version 2.02C を

インストールした上で、下記のセキュリティパッチを適用してください。
MC Works64 Version 2.02C (Version 10.87.148.42)
<MC Works64 Version 1.02C (Version 10.72.088.15)以前品>
当社の支社・代理店にお問い合わせください。
<MC Works32 Version 3.00A 向けセキュリティパッチ>
MC Works32 Version 3.00A (Version 9.50.255.02)

■回避策

上記の対策(ソフトウェアの更新)を事情により実施できない場合、以下の軽減策を実施してください。

(1) 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、信頼できないネットワークやホストからアクセスできないようにします。
(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) リモートアクセスが必要な場合は、接続されたデバイスの安全性を確保するために、仮想プライベートネットワーク(VPN)を使用してください。

■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。

■更新履歴

2021 年 6 月 14 日
・セキュリティパッチをダウンロードできる Web ページの URL を更新しました。
・セキュリティパッチの対象バージョンの誤記を修正しました。

2021 年 1 月 14 日
MC Works64 Version 2.00A～2.02C 向けセキュリティパッチの情報を追加しました。

2020 年 12 月 8 日
MC Works64 Version 3.00A～3.04E 向けセキュリティパッチの情報を追加しました。

2020 年 9 月 9 日
MC Works64 Version 4.00A～4.02C 向けセキュリティパッチの情報を追加しました。