GENESIS64、ICONICS Suite、MobileHMI、Hyper Historian、AnalytiX、MC Works64 及び GENESIS における複数の情報漏えい、改ざん及びサービス拒否(DoS)の脆弱性

公開日 2026 年 4 月 7 日
三菱電機株式会社

■概要

GENESIS64、ICONICS Suite、MobileHMI、Hyper Historian、AnalytiX、MC Works64 及び GENESIS において、複数の情報漏えい、改ざん及びサービス拒否(DoS)の脆弱性が存在することが判明しました。SQLite を利用したローカルキャッシュ機能が有効になっており、かつ SQL サーバーの認証方法に SQL 認証が使用されている場合に、攻撃者は、当該製品がインストールされた PC に格納されているファイルから、当該製品が利用している SQL サーバの認証情報を取得することができる可能性があります(CVE-2025-14815)。また、SQL サーバーの認証方法に SQL 認証が使用されている場合に、当該製品の画面から、当該製品が利用している SQL サーバの認証情報を取得することができる可能性があります(CVE-2025-14816)。結果として、攻撃者は、SQL サーバへ不正にアクセスし SQL サーバ上の情報を窃取又は改ざん・破壊したり、システムをサービス停止(DoS)状態に陥らせることができる可能性があります。

これらの脆弱性の影響を受ける製品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-2025-14815 CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H 基本値:9.3
CVE-2025-14816 CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H 基本値:9.3

■該当製品の確認方法

<該当製品とバージョン>

GENESIS64	:Version 10.97.3 以前のバージョン
ICONICS Suite	:Version 10.97.3 以前のバージョン
MobileHMI	:Version 10.97.3 以前のバージョン
Hyper Historian	:Version 10.97.3 以前のバージョン
AnalytiX	:Version 10.97.3 以前のバージョン
MC Works 64	:全てのバージョン
GENESIS	:Version 11.02 以前のバージョン

<GENESIS64、ICONICS Suite、MobileHMI、Hyper Historian 及び AnalytiX>

Windows のコントロールパネルを開き、「プログラム」>「プログラムと機能」を選択します。
該当製品名※のバージョンに「10.97.306.55」以下が表示されていれば該当します(図 1 参照)。
※Verion 10.96.2 以降の GENESIS64、MobileHMI、Hyper Historian、AnalytiX は ICONICS Suite に同梱されているため、製品名が ICONICS Suite と表示されます。

図1 ICONICS Suite Version 10.97.3

<GENESIS>

Windows のコントロールパネルを開き、「プログラム」>「プログラムと機能」を選択します。
「ICONICS GENESIS」のバージョンに「11.2.394」以下が表示されていれば該当します(図 2 参照)。

図 2 GENESIS Version 11.02

■脆弱性の説明

GENESIS64、ICONICS Suite、MobileHMI、Hyper Historian、AnalytiX、MC Works64 及び GENESIS には、以下 2 件の情報漏えい、改ざん及びサービス拒否(DoS)の脆弱性が存在します。

CVE-2025-14815 該当製品において、SQLite を利用したローカルキャッシュ機能が有効になっており、かつ SQL サーバーの認

[1] https://www.first.org/cvss/v4-0/specification-document

証方法に SQL 認証が使用されている場合に、SQL サーバーの認証情報がローカルの SQLite ファイルに平文で保存されるため、重要な情報の平文保存(CWE-312[2])による、情報漏えい、改ざん及びサービス拒否(DoS)の脆弱性が存在します。

CVE-2025-14816 該当製品の Hyper Historian Splitter 機能において、SQL サーバーの認証方法に SQL 認証が使用されている場合に、SQL サーバーの認証情報が GUI 上に平文で表示されるため、GUI における平文での重要な情報の保存(CWE-317[3])による、情報漏えい、改ざん及びサービス拒否(DoS)の脆弱性が存在します。

■脆弱性がもたらす脅威

攻撃者は、これらの脆弱性を悪用することにより、当該製品が利用している SQL サーバの認証情報を取得することができる可能性があります。結果として、攻撃者は、SQL サーバへ不正にアクセスし SQL サーバ上の情報を窃取又は改ざん・破壊したり、システムをサービス停止(DoS)状態に陥らせることができる可能性があります。

■お客様での対応

CVE-2025-14815

<GENESIS64、ICONICS Suite、MobileHMI、Hyper Historian 及び AnalytiX をご使用中のお客様>

「■製品での対応」に記載されている対策済みの最新の製品をダウンロードし、適用してください。

適用後、「■軽減策・回避策」の「CVE-2025-14815」に記載の軽減策を実施してください。

<MC Works64 をご使用中のお客様>

本脆弱性に対する対策を含むバージョンのリリース予定はございませんので、「■軽減策・回避策」に記載の軽減策にて対応をお願いいたします。

本脆弱性が悪用されるリスクを最小限に抑えるため、以下を参考に GENESIS64 への置き換えをご検討ください。

MC Works64 から GENESIS64 への置き換え

「GENESIS64 – How to replace MC Works64 with GENESIS64_JP」

(https://www.mitsubishielectric.co.jp/dl/fa/members/document/manual/scada/bcn-p5999-1459/bcnp59991459a.pdf)

<GENESIS をご使用中のお客様>

「■製品での対応」に記載されている対策済みの最新の GENESIS をダウンロードし、適用してください。

適用後、「■軽減策・回避策」の「CVE-2025-14815」に記載の軽減策を実施してください。

CVE-2025-14816

<GENESIS64、ICONICS Suite、MobileHMI、Hyper Historian 及び AnalytiX をご使用中のお客様>

「■製品での対応」に記載されている対策済みの最新の GENESIS をダウンロードし、適用してください。

<MC Works64 をご使用中のお客様>

本脆弱性に対する対策を含むバージョンのリリース予定はございませんので、「■軽減策・回避策」に記載の軽減策にて対応をお願いいたします。

本脆弱性が悪用されるリスクを最小限に抑えるため、以下を参考に GENESIS64 への置き換えをご検討ください。

MC Works64 から GENESIS64 への置き換え

「GENESIS64 – How to replace MC Works64 with GENESIS64_JP」

(https://www.mitsubishielectric.co.jp/dl/fa/members/document/manual/scada/bcn-p5999-1459/bcnp59991459a.pdf)

<GENESIS をご使用中のお客様>

「■製品での対応」に記載されている対策済みの最新の GENESIS をダウンロードし、適用してください。

■製品での対応

CVE-2025-14815

<GENESIS64、ICONICS Suite、MobileHMI、Hyper Historian 及び AnalytiX>

Version 10.98 以降で対策済みです。対策済みの最新の製品※は、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

※GENESIS64、MobileHMI、Hyper Historian、及び AnalytiX は、ICONICS Suite に同梱されています。

<MC Works64>

本脆弱性に対する対策を含むバージョンのリリース予定はございません。

<GENESIS>

2 https://cwe.mitre.org/data/definitions/312.html

3 https://cwe.mitre.org/data/definitions/317.html

Version 11.03 以降で対策済みです。対策済みの最新の製品は、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

CVE-2025-14816
Version 10.98 以降で対策済みです。対策済みの最新の製品※は、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

※GENESIS64、MobileHMI、Hyper Historian、及び AnalytiX は、ICONICS Suite に同梱されています。

<MC Works64>
本脆弱性に対する対策を含むバージョンのリリース予定はございません。

<GENESIS>
Version 11.03 以降で対策済みです。対策済みの最新の製品は、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・回避策
上記の対策を実施できない場合には、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。

全ての脆弱性
(1) SQL サーバーの認証方法として SQL 認証ではなく、Windows 認証を使用してください。
(2) 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。
(3) 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。
(4) 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。
(5) 該当製品がインストールされた PC 及び本 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。
(6) 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。

CVE-2025-14815
(1) Workbench の「アプリケーション設定」ダイアログの「利用可能なアプリケーション」にある、「ローカルキャッシュ」列のチェックボックスを外し、ローカルキャッシュ機能により作成されたファイルを以下の保存場所より削除してください。

<GENESIS64、ICONICS Suite、MobileHMI、Hyper Historian 及び AnalytiX での保存場所>
C:¥ProgramData¥ICONICS¥Cache¥*.sdf

<MC Works64 での保存場所>
C:¥ProgramData¥ICONICS¥Cache¥*.sdf

<GENESIS での保存場所>
C:¥ProgramData¥ICONICS¥11¥Cache¥*.sqlite3

CVE-2025-14816
(1) HHSplitter.exe のアクセス許可を変更し、信頼できる管理者のみが実行できるようにしてください。
(2) 不要な場合には、HHSplitter.exe を削除してください。

■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。

<お問い合わせ | 三菱電機 FA>
https://www.mitsubishielectric.co.jp/fa/support/purchase/index.html