

GENESIS、GENESIS64、ICONICS Suite、Hyper Historian、AnalytiX、MobileHMI、IoTWorX、MC Works64、GENESIS32 及び BizViz における複数の脆弱性

公開日 2026 年 10 月 15 日
三菱電機株式会社

■概要

GENESIS、GENESIS64、ICONICS Suite、Hyper Historian、AnalytiX、MobileHMI、IoTWorX、MC Works64、GENESIS32 及び BizViz において、複数の脆弱性が存在することが判明しました。攻撃者は、これらの脆弱性を悪用することにより、任意のコードを実行したり(CVE-2023-4863)、認証を回避したり(CVE-2026-16436 及び CVE-2026-16437)、任意の操作を実行したり(CVE-2026-16438)することができます。その結果、情報の窃取、改ざん、破壊又は削除が行われる又はシステムがサービス停止(DoS)状態に陥る恐れがあります。

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。修正版に更新するか、軽減策を適用してください。

■CVSS スコア¹

CVE-2023-4863	CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H	Base Score:9.3
CVE-2026-16436	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N	Base Score:9.2
CVE-2026-16437	CVSS:4.0/AV:L/AC:H/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N	Base Score:7.1
CVE-2026-16438	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H	Base Score:9.4

■該当製品の確認方法

該当製品及びバージョンは以下のとおりです。

CVE ID	製品名	バージョン
CVE-2023-4863	GENESIS64	10.97 から 10.97.2
	ICONICS Suite	10.97 から 10.97.2
CVE-2026-16436 、 CVE-2026-16437	GENESIS	11.03 以前
	GENESIS64	10.97.3 以前
	ICONICS Suite	10.97.3 以前
	Hyper Historian	10.97.3 以前
	AnalytiX	10.97.3 以前
	MobileHMI	10.97.3 以前
	IoTWorX	10.97.3 以前
	MC Works64	全バージョン
	GENESIS32	全バージョン
	BizViz	全バージョン
CVE-2026-16438	GENESIS64	10.97.3 以前
	ICONICS Suite	10.97.3 以前
	Hyper Historian	10.97.3 以前
	AnalytiX	10.97.3 以前
	MobileHMI	10.97.3 以前
	MC Works64	全バージョン

＜バージョンの確認方法(Windows 11)＞

- 1) 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。
- 2) GENESIS をご利用のお客様の場合には、名前に「GENESIS」と表示され、バージョンが「11.3.578」以前であれば該当します(図 1 参照)。

名前	発行元	インストール日	サイズ	バージョン
GENESIS	ICONICS	2026/09/29	9.66 GB	11.3.578

図 1 GENESIS Version 11.03

- 3) GENESIS64 又は ICONICS Suite をご利用のお客様の場合には、名前に「ICONICS Suite※」と表示され、バージョンが「10.97.020.27」から「10.97.212.46」までであれば該当します(図 2 参照)。

※GENESIS64 はインストール時に ICONICS Suite に同梱されるため、名前は「ICONICS Suite」と表示されます。

¹ <https://www.first.org/cvss/v4-0/specification-document>

名前 ICONICS Suite	発行元 ICONICS	バージョン 10.97.212.46
---------------------	----------------	-----------------------

図 2 ICONICS Suite Version 10.97.2

- 4) GENESIS64、ICONICS Suite、Hyper Historian、AnalytiX、MobileHMI 又は IoTWorX をご利用のお客様の場合には、名前に「ICONICS Suite※」と表示され、バージョンが「10.97.306.55」以前であれば該当します(図 3 参照)。

※GENESIS64、MobileHMI、Hyper Historian 及び AnalytiX はインストール時に ICONICS Suite に同梱されるため、名前は「ICONICS Suite」と表示されます。

名前 ICONICS Suite	発行元 ICONICS	インストール日 2025/12/6	サイズ 2.73GB	バージョン 10.97.306.55
---------------------	----------------	----------------------	---------------	-----------------------

図 3 ICONICS Suite Version 10.97.3

脆弱性の説明

GENESIS、GENESIS64、ICONICS Suite、Hyper Historian、AnalytiX、MobileHMI、IoTWorX、MC Works64、GENESIS32 及び BizViz には以下 4 件の脆弱性が存在します。

CVE ID	脆弱性の説明
CVE-2023-4863	GENESIS64 及び ICONICS Suite において、内部コンポーネントである libwebp に起因する境界外書き込み (CWE-787 ²) による任意のコードが実行される脆弱性が存在します。
CVE-2026-16436	GENESIS、GENESIS64、ICONICS Suite、Hyper Historian、AnalytiX、MobileHMI、IoTWorX、MC Works64、GENESIS32 及び BizViz において、パスワードを忘れた場合の脆弱なパスワードリカバリの仕組み (CWE-640 ³) による認証回避の脆弱性が存在します。該当製品のセキュリティチャレンジ機能では、システムのロックを解除するために使用されるチャレンジレスポンスが、全てのユーザーで共通かつ固定値です。そのため、チャレンジレスポンスを入手すれば、誰でもシステムのロックを解除できます。
CVE-2026-16437	GENESIS、GENESIS64、ICONICS Suite、Hyper Historian、AnalytiX、MobileHMI、IoTWorX、MC Works64、GENESIS32 及び BizViz において、パスワードを忘れた場合の脆弱なパスワードリカバリの仕組み (CWE-640) に起因する認証回避の脆弱性が存在します。該当製品のセキュリティチャレンジ機能では、管理者が、システムのロック解除に使用されるチャレンジレスポンスを保存した、Windows によって保護されている管理ファイルを読み書きできます。
CVE-2026-16438	GENESIS64、ICONICS Suite、Hyper Historian、AnalytiX、MobileHMI 及び MC Works64 において、不適切な権限設定 (CWE-266 ⁴) による任意の操作が実行される脆弱性が存在します。該当製品のインストーラーは、インストール時に、製品の管理者アカウントに対して不要な既定の DCOM 権限を付与します。その結果、これらの管理者アカウントを持つユーザーは、本来 UAC による権限昇格が必要な DCOM オブジェクトを、ローカル又はリモートから起動及び操作できる可能性があります。

脆弱性がもたらす脅威

本脆弱性が悪用された場合には、情報の窃取、改ざん、破壊又は削除が行われる又はシステムがサービス停止 (DoS) 状態に陥る可能性があります。

CVE ID	脆弱性がもたらす脅威
CVE-2023-4863	PC にローカルログインした攻撃者が、細工したファイルを該当製品の管理者としてインポートすることにより、ヒープベースのバッファオーバーフローを引き起こし、任意のコードを実行できる可能性があります。その結果、攻撃者は、内部情報を窃取や改ざん、破壊、削除したり、影響を受けるシステムをサービス停止 (DoS) 状態に陥らせたりする可能性があります。
CVE-2026-16436	リモートの攻撃者が、何らかの手段でチャレンジレスポンスを入手することにより、システムのロックを解除できる可能性があります。その結果、攻撃者は、内部情報を窃取や改ざん、破壊、削除したり、影響を受けるシステムをサービス停止 (DoS) 状態に陥らせたりする可能性があります。
CVE-2026-16437	管理者権限で PC にローカルログインした攻撃者が、チャレンジレスポンスを保存している管理ファイルを改ざんすることにより、システムのロックを解除できる可能性があります。その結果、攻撃者は、内部情報を窃取や改ざん、破壊、削除したり、影響を受けるシステムをサービス停止 (DoS) 状態に陥らせたりする可能性があります。

² <https://cwe.mitre.org/data/definitions/787.html>

³ <https://cwe.mitre.org/data/definitions/640.html>

⁴ <https://cwe.mitre.org/data/definitions/266.html>

CVE ID	脆弱性がもたらす脅威
CVE-2026-16438	該当製品で使用されている管理者アカウントを使ってログインできる攻撃者は、DCOM オブジェクトをローカル又はリモートから起動及び操作できる可能性があります。その結果、攻撃者は、内部情報を窃取や、改ざん、破壊、削除したり、影響を受けるシステムをサービス停止 (DoS) 状態に陥らせたりする可能性があります。

■お客様での対応

GENESIS、GENESIS64、ICONICS Suite、Hyper Historian、AnalytiX、MobileHMI 及び IoTWorX をご利用のお客様は、「製品での対応」に記載されている修正版をダウンロードしてインストールしてください。該当製品を継続して使用する必要があるお客様には、「軽減策・回避策」に記載されている対応を実施することを推奨します。

MC Works64 の修正版をリリースする予定がないため、MC Works64 をご利用のお客様には、「軽減策・回避策」に記載されている対応を実施することを推奨します。または、GENESIS64 又は GENESIS への置き換えをご検討ください。置き換え方法については、以下の資料を参照してください。

「MC Works64 から GENESIS64 への置き換え」

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

注: この資料は当社の FA サイトで公開されており、閲覧には会員登録及びログインが必要です。

GENESIS32 及び BizViz の修正版をリリースする予定がないため、GENESIS32 及び BizViz をご利用のお客様には、「軽減策・回避策」に記載されている対応を実施することを推奨します。または、GENESIS64 又は GENESIS への置き換えをご検討ください。

■製品での対応

以下の製品では、本脆弱性への対策が行なわれています。

CVE ID	製品名	修正済みバージョン及びインストール入手方法
CVE-2023-4863	GENESIS64 及び ICONICS Suite	ICONICS Suite バージョン 10.97.3 以降で対策済みです。 以下のリンクからダウンロードしてインストールしてください。 https://iconicsinc.my.site.com/community/s/resource-center/product-downloads 注: GENESIS64 は、ICONICS Suite のインストールに含まれています。
CVE-2026-16436 、 CVE-2026-16437	GENESIS64、ICONICS Suite、 Hyper Historian、AnalytiX 及び MobileHMI	ICONICS Suite バージョン 10.98 以降で対策済みです。 以下のリンクからダウンロードしてインストールしてください。 https://iconicsinc.my.site.com/community/s/resource-center/product-downloads 注: GENESIS64、Hyper Historian、AnalytiX 及び MobileHMI は、 ICONICS Suite のインストールに含まれています。
	IoTWorX	IoTWorX バージョン 10.98 以降で対策済みです。 以下のリンクからダウンロードしてインストールしてください。 https://hub.docker.com/r/iconics/iotworx
	GENESIS	GENESIS バージョン 11.04 以降で対策済みです。 以下のリンクからダウンロードしてインストールしてください。 https://iconicsinc.my.site.com/community/s/resource-center/product-downloads
CVE-2026-16438	GENESIS64、ICONICS Suite、 Hyper Historian、AnalytiX 及び MobileHMI	ICONICS Suite バージョン 10.98 以降で対策済みです。 以下のリンクからダウンロードしてインストールしてください。 https://iconicsinc.my.site.com/community/s/resource-center/product-downloads 注: GENESIS64、Hyper Historian、AnalytiX 及び MobileHMI は、 ICONICS Suite のインストールに含まれています。

■軽減策・回避策

三菱電機は、本脆弱性が悪用されるリスクを最小限に抑えるため、お客様に以下の軽減策や回避策を実施することを推奨します。

全ての脆弱性

- (1) 該当製品がインストールされている 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。
- (2) 該当製品がインストールされている 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ーからのリモートログインをブロックしてください。
- (3) 該当製品がインストールされている 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、仮想プライベートネットワーク(VPN)などを使用して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てください。
- (4) 該当製品がインストールされている PC 及びその 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てください。
- (5) 信頼できない送信元からのメールに記載された Web リンクをクリックしないでください。また、信頼できないメールの添付ファイルを開かないでください。

CVE-2023-4863

- (1) 該当製品がインストールされている PC にウイルス対策ソフトをインストールしてください。

CVE-2026-16436 及び CVE-2026-16437

- (1) 該当製品がインストールされている PC にウイルス対策ソフトをインストールしてください。
- (2) GENESIS、GENESIS64、ICONICS Suite、Hyper Historian、AnalytiX、MobileHMI 及び MC Works64 に対して、以下の手順を実施してください。
 - 1) 以下に指定する場所にある.dat ファイルを削除してください。このファイル名及び保存場所は、製品のバージョンによって異なります。
バージョン 10: C:\Program Files\ICONICS\GENESIS64\Components\ClientChallengeTable.dat
バージョン 11: C:\ProgramData\ICONICS\11\SecurityChallenges.dat
 - 2) 同じファイル名及び保存場所で、空のファイルを作成してください。
 - 3) このファイルに対するファイルシステムの書き込み及び削除のアクセス権を、GENESIS の管理者アカウントとは異なる専用の管理者アカウントに制限してください。

CVE-2026-16438

- (1) 該当製品がインストールされている PC を LAN 内で使用し、信頼できないネットワークやホストからのアクセスを、ファイアウォールでブロックしてください。
- (2) 該当製品がインストールされている PC をインターネットに接続する場合は、ファイアウォール、仮想プライベートネットワーク(VPN)などを使用して不正アクセスを防止してください。
- (3) 該当製品がインストールされている PC 及びその PC にアクセス可能な全ての PC に、ウイルス対策ソフトをインストールしてください。

■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>