



公開日：2024/07/04 最終更新日：2026/04/07

## JVNVU#98894016 三菱電機製複数製品における複数の脆弱性

### 概要

三菱電機株式会社が提供するGENESIS64、ICONICS Suite、Hyper Historian、AnalytiX、MobileHMI、IoTWorX、MC Works64、GENESIS32およびBizVizには、複数の脆弱性が存在します。

### 影響を受けるシステム

#### CVE-2023-2650

- GENESIS64 Version 10.97.2
- ICONICS Suite Version 10.97.2
- Hyper Historian Version 10.97.2
- AnalytiX Version 10.97.2
- MobileHMI Version 10.97.2

#### CVE-2023-4807

- GENESIS64 Version 10.97.2
- ICONICS Suite Version 10.97.2
- Hyper Historian Version 10.97.2
- AnalytiX Version 10.97.2
- MobileHMI Version 10.97.2

#### CVE-2024-1182

- GENESIS64 Version 10.97.3およびそれ以前のバージョン
- ICONICS Suite Version 10.97.3およびそれ以前のバージョン
- Hyper Historian Version 10.97.3およびそれ以前のバージョン
- MC Works64 全バージョン
- GENESIS32 Version 9.7およびそれ以前のバージョン

#### CVE-2024-1573

- GENESIS64 Version 10.97.2およびそれ以前のバージョン
- ICONICS Suite Version 10.97.2およびそれ以前のバージョン
- Hyper Historian Version 10.97.2およびそれ以前のバージョン
- AnalytiX Version 10.97.2およびそれ以前のバージョン
- MobileHMI Version 10.97.2およびそれ以前のバージョン
- IoTWorX Version 10.95
- MC Works64 全バージョン

#### CVE-2024-1574

## JVN

[HOME](#)
[JVNとは](#)
[脆弱性レポートの読み方](#)
[脆弱性レポート一覧](#)
[VN-JP](#)
[VN-JP \(調整不能\)](#)
[VN-VU](#)
[TA](#)
[TRnotes](#)
[JVN iPedia](#)
[脆弱性対策情報データベース](#)
[MyJVN](#)
[JVNS/RSS](#)
[ベンダ情報一覧](#)
[連絡不能開発者一覧](#)
[脆弱性情報の届出](#)
[お問合せ先](#)

- GENESIS64 Version 10.97.2およびそれ以前のバージョン
- ICONICS Suite Version 10.97.2およびそれ以前のバージョン
- Hyper Historian Version 10.97.2およびそれ以前のバージョン
- AnalytiX Version 10.97.2およびそれ以前のバージョン
- MobileHMI Version 10.97.2およびそれ以前のバージョン
- MC Works64 全バージョン
- GENESIS32 Version 9.7およびそれ以前のバージョン
- BizViz Version 9.7およびそれ以前のバージョン

バージョンの確認方法等の詳細については、開発者が提供する情報を確認してください。

## 詳細情報

三菱電機株式会社が提供するGENESIS64、ICONICS Suite、Hyper Historian、AnalytiX、MobileHMI、IoTWorX、MC Works64、GENESIS32およびBizVizには、次の複数の脆弱性が存在します。

- **制限または上限なしのリソースの割り当て (CWE-770)**
  - CVSS:v3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L 基本値: 3.7
  - 当該製品に組み込まれているOpenSSLの脆弱性 (CVE-2023-2650) に起因しています
- **デジタル署名の不適切な検証 (CWE-347)**
  - CVSS:v3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H 基本値: 5.9
  - 当該製品に組み込まれているOpenSSLの脆弱性 (CVE-2023-4807) に起因しています
- **ファイル検索パスの制御不備 (CWE-427)**
  - CVSS:v3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H 基本値: 7.0
  - CVE-2024-1182
- **重要な機能に対する認証の欠如 (CWE-306)**
  - CVSS:v3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N 基本値: 5.9
  - CVE-2024-1573
- **安全でないリフレクション (CWE-470)**
  - CVSS:v3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H 基本値: 6.7
  - CVE-2024-1574

## 想定される影響

想定される影響は各脆弱性により異なりますが、次のような可能性があります。

### CVE-2023-2650

OpenSSLを使用しているBACnetセキュア通信機能が、攻撃者によって細工されたASN.1オブジェクト識別子を含む証明書を受信し検証することで、一時的にサー

ビス運用妨害 (DoS) 状態となる

#### CVE-2023-4807

OpenSSLを使用しているBACnetセキュア通信機能が、攻撃者によって細工されたメッセージ認証コード (MAC) を含むメッセージを受信し、処理することで、サービス運用妨害 (DoS) 状態となる

#### CVE-2024-1182

攻撃者が細工したDLLファイルを特定のフォルダに格納することで、悪意あるプログラムが実行される

#### CVE-2024-1573

攻撃者によって適切な認証を回避され、システムにログインされる

#### CVE-2024-1574

システムによって保護されていない特定のファイルを攻撃者により書き換えられることで、悪意あるプログラムを管理者権限で実行される

詳しくは、開発者が提供する情報を確認してください。

### 対策方法

#### アップデートする

アップデートが提供されている製品に関しては、開発者が提供する情報をもとに最新版にアップデートしてください。

#### アップグレードするまたは後続製品・バージョンへ移行する

一部の製品に関しては、開発者は後継製品へのアップグレードを推奨しています。

対象製品等の詳細については、開発者が提供する情報を確認してください。

#### ワークアラウンドを実施する

アップデートが提供されていない製品や、後続製品へのアップグレードが難しい場合に関しては、開発者が提供する緩和策および軽減策を適用してください。各脆弱性向けの具体的な緩和策および軽減策の詳細については、開発者が提供する情報を確認してください。

### ベンダ情報

ベンダ リンク

三菱電機  
株式会社

[GENESIS64](#)、[ICONICS Suite](#)、[Hyper Historian](#)、[AnalytiX](#)、[MobileHMI](#)、[IoTWorX](#)、[MC Works64](#)、[GENESIS32](#)および[BizViz](#)における複数の脆弱性

### 参考情報

1. [JVNVU#94584169](#)

OpenSSLのASN.1 オブジェクト識別子変換における処理時間遅延の問題 (Security Advisory [30th May 2023])

2. [JVNVU#96140980](#)

OpenSSLのPOLY1305 MAC実装におけるWindows上のXMMレジスタが破

損する問題 (Security Advisory [8th September 2023])

### 3. ICS Advisory | ICSA-24-184-03

ICONICS and Mitsubishi Electric Products

---

## JPCERT/CCからの補足情報

---

## JPCERT/CCによる脆弱性分析結果

---

### 謝辞

この脆弱性情報は、製品利用者への周知を目的に、開発者がJPCERT/CCに報告し、JPCERT/CCが開発者との調整を行いました。

---

### 関連文書

JPCERT 緊急報告

JPCERT REPORT

CERT Advisory

CPNI Advisory

TRnotes

CVE

JVN iPedia

---

### 更新履歴

#### 2026/01/08

[タイトル]、[概要]、[影響を受けるシステム]、[詳細情報]、[対策方法]、[ベンダ情報]を更新しました

#### 2026/04/07

[タイトル]、[概要]、[影響を受けるシステム]、[詳細情報]、[対策方法]、[ベンダ情報]を更新しました

Copyright (c) 2000-2026 JPCERT/CC and IPA. All rights reserved.