公開日：2024/11/28　最終更新日：2026/04/07

JVNVU#93891820
三菱電機製複数製品における複数の脆弱性

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
JVNJS/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

概要

三菱電機製GENESIS64、ICONICS Suite、Hyper Historian、MC Works64およびGENESIS32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-2024-8299

- 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
- GENESIS32 全バージョン
- MC Works64 全バージョン

CVE-2024-8300

- GENESIS64 Version 10.97.2、10.97.2 CFR1、10.97.2 CFR2、10.97.3
- ICONICS Suite Version 10.97.2、10.97.2 CFR1、10.97.2 CFR2、10.97.3

CVE-2024-9852

- 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
- Hyper Historian Version 10.97.3以前のバージョン
- GENESIS32 すべてのバージョン
- MC Works64 すべてのバージョン

影響を受けるバージョンの確認方法等の詳細は、開発者が提供する情報を確認してください。

詳細情報

三菱電機製GENESIS64、ICONICS Suite、Hyper Historian、MC Works64およびGENESIS32には、次の複数の脆弱性が存在します。

- **ファイル検索パスの制御不備（CWE-427）**
  - CVSS:v3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H 基本値: 7.8
  - CVE-2024-8299
- **デッドコード（CWE-561）**
  - 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-2024-8300
- **ファイル検索パスの制御不備（CWE-427）**

- CVSS:v3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H 基本値: 7.8
- CVE-2024-9852

想定される影響

CVE-2024-8299、CVE-2024-9852
細工されたDLLを特定のフォルダに格納された場合、悪意のあるプログラムが実行され、当該製品上の情報の漏えいや改ざん、破壊、削除をされたり、当該製品がサービス運用妨害（DoS）状態にされたりする可能性があります。

CVE-2024-8300
特定のDLLを改ざんされた場合、悪意のあるプログラムが実行され、当該製品上の情報の漏えいや改ざん、破壊、削除をされたり、当該製品がサービス運用妨害（DoS）状態にされたりする可能性があります。

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。

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。

- 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、ユーザからのリモートログインをブロックする
- 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、信頼できるユーザのみにリモートログインを許可する
- 該当製品がインストールされたPCおよび本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する
- 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、また信頼できないメールに添付されたファイルを開かない

詳しくは、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、MC Works64およびGENESIS32における複数の脆弱性

参考情報

1. ICS Advisory | ICSA-24-338-04
   ICONICS and Mitsubishi Electric GENESIS64 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

2024/12/04

［参考情報］にICS Advisoryのリンクを追加しました

2025/01/16

［影響を受けるシステム］、［想定される影響］、［対策方法］を更新しました

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