



公開日：2026/04/07 最終更新日：2026/04/07

## JVNVU#90646130

### 複数の三菱電機製品における重要情報の平文保存の脆弱性

#### 概要

複数の三菱電機製品には、重要情報の平文保存の脆弱性が存在します。

#### 影響を受けるシステム

- 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
- MobileHMI
  - 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
- AnalytiX
  - 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
- GENESIS
  - Version 11.02およびそれ以前のバージョン

#### 詳細情報

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

- 重要な情報の平文保存 (CWE-312)
  - CVE-2025-14815
  - 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本脆弱性の影響を受けます
- GUIでの重要な情報の平文保存 (CWE-317)
  - CVE-2025-14816

## 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 脆弱性対象情報データベース	
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	

- 当該製品の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本脆弱性の影響を受けます

---

### 想定される影響

攻撃者によりSQLサーバーの認証情報が窃取され、結果として、情報漏えい、情報改ざん、サービス運用妨害（DoS）が行われる可能性があります。

---

### 対策方法

#### CVE-2025-14815向け対策：

##### アップデートを適用後、軽減策・回避策を実施する

GENESIS64、ICONICS Suite、MobileHMI、Hyper Historian、AnalytiX、GENESISに関しては、対策済の最新版を使用し、その後開発者が提示するCVE-2025-14815向けの「軽減策・回避策」を実施してください。

##### 製品の置き換えもしくは軽減策・回避策を実施する

MC Works64に関しては、対策版の提供予定はありません。

MC Works64からGENESIS64への置き換えを実施するか、開発者が提示するCVE-2025-14815向けの「軽減策・回避策」を実施してください。

#### CVE-2025-14816向け対策：

##### アップデートする

GENESIS64、ICONICS Suite、MobileHMI、Hyper Historian、AnalytiX、GENESISに関しては、対策済の最新版を使用してください。

なお、MC Works64に関しては、対策版の提供予定はありません。

アップデート、製品の置き換え、軽減策・回避策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。

---

### ベンダ情報

ベンダ リンク

三菱電機株式会社	<a href="#">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</a>
----------	---------------------------------------------------------------------------------------------------------------------------------

---

### 参考情報

[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](#)

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