公開日：2025/05/20　最終更新日：2026/04/07

JVNVU#93838985
三菱電機製複数製品の複数のサービス実行時に必要以上に高い権限が割り当てられている脆弱性

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、MobileHMI、Hyper Historian、AnalytiX、IoTWorX、MC Works64、GENESIS、GENESIS32およびBizVizの複数のサービスは、必要以上に高い権限で実行されています。

影響を受けるシステム

- 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
- IoTWorX Version 10.95
- MC Works64 全バージョン
- GENESIS32 全バージョン
- BizViz 全バージョン
- GENESIS Version 11.00

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
三菱電機製GENESIS64、ICONICS Suite、MobileHMI、Hyper Historian、AnalytiX、IoTWorX、MC Works64、GENESIS、GENESIS32およびBizVizの複数のサービスは、必要以上に高い権限で実行されています（CWE-250、CVE-2025-0921）。

想定される影響
攻撃者は、該当製品のサービスが書き込み先として使用するファイルから攻撃対象のファイルへのシンボリックリンクを作成することで、任意のファイルへの不正な書き込みを可能にします。結果として、攻撃者は、該当製品がインストールされたPC上のファイルを、破壊できる可能性があります。破壊されたファイルが当該PCの動作に必要なファイルの場合、当該PCがサービス運用妨害（DoS）状態とな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。
開発者が提供する情報をもとに最新版をダウンロードし適用してください。

ワークアラウンドを実施する
アップデートが提供されない製品に関しては、開発者が提供する情報をもとに回避策・軽減策を適用してください。

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、MobileHMI、Hyper Historian、AnalytiX、IoTWorX、MC Works64、GENESIS、GENESIS32及びBizVizの複数のサービスにおける情報改ざんの脆弱性

参考情報

1. ICS Advisory | ICSA-25-140-04
   Mitsubishi Electric Iconics Digital Solutions 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

2025/05/21
［参考情報］にICS Advisoryのリンクを追加しました

2025/08/05
［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

2026/01/08

［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