FANUC MT-LINKi/ROBODRILL-LINKi に搭載された MongoDB における情報漏えいの可能性がある脆弱性について

公開日 2026 年 2 月 25 日
ファナック株式会社

■ 概要

当社製 FANUC MT-LINKi/ROBODRILL-LINKi で使用されているデータベース MongoDB において、脆弱性があることが判明しました。これらの脆弱性を攻撃者に悪用された場合、MongoDB 内の機密情報（認証情報など）が漏えいし、収集した稼働情報などが流出する可能性があります。本脆弱性の影響を受ける商品をご使用の場合は、以下に記されている対策の実施をお願いいたします。また、ファイアウォール、アンチウィルスソフト、ネットワークセグメンテーションのセキュリティ制御などのシステム全体に対するセキュリティ対策を、予防・検出・対応制御の一部として推奨します。

■ 影響を受ける商品

MT-LINKi 3.7 版以降
ROBODRILL-LINKi 3.7 版以降

■ 脆弱性の説明

FANUC MT-LINKi／ROBODRILL-LINKi に搭載された MongoDB の脆弱性は、以下のように公表されています。

CVE番号 / CVSSスコア	説明
CVE-2025-14847 CVSS v3.1 基本値：7.5 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N CNA:MongoDB, Inc.	圧縮方法zlibを使用した通信でアクセスした場合、初期化されていないヒープメモリ内に残っている情報を読み取り、MongoDB内の機密情報（認証情報など）が漏えいする可能性がある。

■ 想定される影響

攻撃者に悪用された場合、MongoDB 内の機密情報（認証情報など）が漏えいし、収集した稼働情報などが流出する可能性があります。

■ 対策方法

1. 暫定対策

以下の 2 つの対策をご検討ください。
なお、両方の対策実施を推奨いたしますが、無理な場合には片方でも対策をご検討ください。

・対策 1

[外部通信のブロック]

ファイアウォールの設定で、MongoDB が使用するポート（デフォルトは 27017）へのアクセスを、内部通信（localhost）に制限してください。

・対策 2

[圧縮方法 zlib の除外]

通信の圧縮方法から、脆弱性が含まれている圧縮方法 zlib を除外してください。

圧縮方法 zlib を除外するには、MongoDB 登録コマンドのオプションを変更し、MongoDB サービスを再登録する必要があります。

MongoDB サービスの再登録方法については、テクニカルレポート TMN26/015 の「FANUC MT-LINKi のデータベース MongoDB における脆弱性（CVE-2025-14847）への対策について」をご参照ください。

なお、テクニカルレポートの提供は、担当セールス、サービス、または販売元へご依頼ください。また、MyFANUC にて公開済みです。

2. 恒久対策

CVE-2025-14847 対策済み MongoDB を搭載した MT-LINKi 4.2 版、ROBODRILL-LINKi 4.2 版を、2026 年 3 月にリリースする予定です。MT-LINKi 4.2 版、ROBODRILL-LINKi 4.2 版は MyFANUC にて公開予定です。

また、今回確認された脆弱性に限らず、システム全体において適切なセキュリティ対策を講じていただくことを推奨いたします。

■ 問い合わせ先

担当セールス、サービス、または販売元へお問い合わせいただくか、
ファナックホームページの「お問い合わせメール」にて、お問い合わせください。
https://www.fanuc.co.jp/ja/contact/form/
（“商品の脆弱性に関するお問い合わせ”を選択）

■ 更新履歴

版数	年月日	内容
01	2026-02-25	初版公開