A Vulnerability in MongoDB Incorporated in FANUC MT-LINKi / ROBODRILL-LINKi that May Potentially Lead to Information Leakage

Publication Date 2026-02-25
FANUC CORPORATION

■ Overview

A vulnerability has been identified in the MongoDB database used in our FANUC MT-LINKi and ROBODRILL-LINKi products. If this vulnerability is exploited by an attacker, confidential information stored in MongoDB (such as authentication data) may be exposed, and collected operational data may also be leaked. If you are using a product affected by this vulnerability, please implement the countermeasures described below. In addition, we recommend establishing security controls for the entire system—such as firewalls, antivirus software, and network segmentation—as part of your preventive, detective, and responsive security measures.

■ Affected products

MT-LINKi 3.7 version or later
ROBODRILL-LINKi 3.7 version or later

■ Vulnerability description

The vulnerability in MongoDB incorporated in FANUC MT-LINKi and ROBODRILL-LINKi has been disclosed as described below.

CVE Number / CVSS Score	Description
CVE-2025-14847 CVSS v3.1 Base score : 7.5 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N CNA:MongoDB, Inc.	If accessed using communication that uses the zlib compression method, information remaining in uninitialized heap memory may be read, potentially leaking confidential information (such as authentication information) within MongoDB.

■ Impact

If exploited by an attacker, confidential information stored in MongoDB (such as authentication data) may be exposed, and collected operational data may also be leaked.

■ Countermeasures

1. Temporary countermeasures
   Please consider implementing the following two countermeasures.
   While we recommend implementing both, if that is not feasible, please consider implementing at least one of them.

   ・Countermeasure 1
   [Block External Communication]
   Configure the firewall to restrict access to the port used by MongoDB (default: 27017) to internal communication (localhost).

   ・Countermeasure 2
   [Exclude zlib Compression Method]
   Exclude the zlib compression method, which contains the vulnerability, from the communication compression methods.
   To exclude the zlib compression method, you must change the options in the MongoDB registration command and re-register the MongoDB service.
   For information on how to re-register the MongoDB service, please refer to Technical Report TMN26/015, "Countermeasures for vulnerability (CVE-2025-14847) in MongoDB database of FANUC MT-LINKi."
   Please request the technical report through your sales representative, service personnel, or distributor. It has also been published on MyFANUC.

2. Permanent countermeasures
   We plan to release MT-LINKi Version 4.2 and ROBODRILL-LINKi Version 4.2, which incorporate MongoDB with the CVE-2025-14847 fix, in March 2026. Both MT-LINKi Version 4.2 and ROBODRILL-LINKi Version 4.2 are scheduled to be made available on MyFANUC.

We also recommend implementing appropriate security measures across your entire system, not limited to the vulnerabilities identified in this case.

■ Contact information

Please contact your sales representative, service personnel, or distributor, or submit an inquiry through the “Mail Form” on the FANUC website.
https://www.fanuc.co.jp/en/contact/form/
(Select “Vulnerability Information related to Product Security”)

Revision history

Version	Date	Comments
01	2026-02-25	Initial publication