

MongoDB における情報漏えいの脆弱性（CVE-2025-14847）

1. 脆弱性の概要

M o n g o D B について、次の脆弱性が存在します。

- ・ 認証されていない遠隔の第三者が細工した通信を送信することで、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、結果的に MongoDB 内の機密情報（API キー、認証情報など）が漏えいする可能性があります。

2. 当社製品への影響

本脆弱性の当社製品への影響に関して、以下の表 1～3 に示します。

表 1 ネットワーク装置 1

| 製品名                                       | OS 名称        | 該当非 |
|---|--------------|-----|
| ApresiaCA220 シリーズ                         | AMIOS10      | 非該当 |
| ApresiaCA120 シリーズ                         | AMIOS9       |     |
| Apresia26000 シリーズ                         | AMIOS6       |     |
| Apresia26010QC シリーズ                       | AMIOS6       |     |
| Apresia22000 シリーズ                         | AMIOS7       |     |
| Apresia20000 シリーズ                         | AMIOS7       |     |
| Apresia18000 シリーズ                         | AMIOS2       |     |
| Apresia16000 シリーズ                         | AMIOS3       |     |
| Apresia12000 シリーズ                         | AMIOS5       |     |
| Apresia13000, 15000 シリーズ                  | AEOS8        |     |
| Apresia2000, 3000, 4000, 5000, 13000 シリーズ | AEOS7, AEOS6 |     |
| ApresiaNP7000 シリーズ                        | AEOS-NP7000  |     |
| ApresiaNP5000 シリーズ                        | AEOS-NP5000  |     |
| ApresiaNP4000 シリーズ                        | AEOS-NP4000  |     |
| ApresiaNP3000 シリーズ                        | AEOS-NP3000  |     |
| ApresiaNP2500 シリーズ                        | AEOS-NP2500  |     |
| ApresiaNP2100 シリーズ                        | AEOS-NP2100  |     |
| ApresiaNP2000 シリーズ                        | AEOS-NP2000  |     |
| ApresiaLight FM シリーズ                      | APLFMOS      |     |
| ApresiaLight GM シリーズ                      | APLGMOS      |     |
| ApresiaLight GM200 シリーズ                   | APLGM200OS   |     |
| ApresiaLight GM300 シリーズ                   | APLGM300OS   |     |
| ApresiaLight GS シリーズ                      | APLGSOS      |     |

表 2 ネットワーク装置 2

| 製品名                    | OS 名称         | 該当<br>非該当 |
|------------------------|---------------|-----------|
| ApresiaLight MC シリーズ   | APLMCOS       | 非該当       |
| ApresiaCAMC-101GT シリーズ | CAMCOS        |           |
| ApresiaCAMC-101X シリーズ  | CAMCOS        |           |
| PONU シリーズ              | PONUWare      |           |
| XGMC シリーズ              | －             |           |
| GMC シリーズ               | －             |           |
| KOKOMO-VPN             | －             | 該当        |
| A3CloudSIM コネクト        | closip エージェント | 非該当       |

表 3 ネットワーク管理システム

| ソフトウェア名             | 該当<br>非該当 |
|---------------------|-----------|
| AP4-GTP-pBroker     | 非該当       |
| ANRC シリーズ           |           |
| HCL Manager Station |           |
| ApresiaManager      |           |
| MMRPManager         |           |
| Command Navigator   |           |
| ApresiaManager/C    |           |
| FCRPManager/C       |           |
| GMXManager          |           |
| GMAManager          |           |
| XLGMCManager        |           |
| OSWManager          |           |
| BMCManager          |           |
| OAM-LB Navigator    |           |
| BFSManager          |           |

### 3. 対策

非該当の場合は不要です。

KOKOMO コアの LAN 側に対して、該当する脆弱性をついた攻撃が行われた場合、KOKOMO 内部のデータが漏洩する可能性がございます。KOKOMO コアの WAN 側(インターネット側)からの影響はございません。

対策として、下記バージョンのリリース予定です。

KOKOMO-VPN : 1.2.2(2026/01 未予定)

KOKOMO-VPN : 1.3.3(2026/01 未予定)

KOKOMO-VPN : 1.4.1(2026/01 未予定)

### 4. 改訂履歴

2026/1/21 初版

以上