

Apache Tomcat partial PUT におけるリモートコード実行、  
情報漏えいや改ざんの脆弱性 (CVE-2025-24813)

1. 脆弱性の概要

Apache Tomcat の partial PUT の元の実装には、次の脆弱性が存在します。

- (1) 特定の条件下で、リモートコード実行、セキュリティ上重要なファイルの表示やコンテンツ挿入の可能性がある

2. 当社製品への影響

本脆弱性の当社製品への影響有無に関して、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        | 影響の有無 |
|-------------------------------------------|--------------|-------|
| Apresia26000 シリーズ                         | AMIOS6       | 非該当   |
| 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                   | APLGM2000S   |       |
| ApresiaLight GM300 シリーズ                   | APLGM3000S   |       |
| ApresiaLight GS シリーズ                      | APLGSOS      |       |

表 2 ネットワーク装置 2

| 製品名             | OS 名称         | 影響の有無 |
|-----------------|---------------|-------|
| PONU シリーズ       | PONUWare      | 非該当   |
| APLMC シリーズ      | APLMCOS       |       |
| XGMC シリーズ       | -             |       |
| GMC シリーズ        | -             |       |
| BMC シリーズ        | -             |       |
| KOKOMO          | -             |       |
| A3CloudCNM      | -             | 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             | 影響の有無 |
|---------------------|-------|
| AP4-GTP-pBroker     | 非該当   |
| ANRC シリーズ           | 該当    |
| HCL Manager Station | 非該当   |
| ApresiaManager      |       |
| MMRPManager         |       |
| Command Navigator   |       |
| ApresiaManager/C    |       |
| FCRPManager/C       |       |
| GMXManager          |       |
| GMAManager          |       |
| XLGMCManager        |       |
| OSWManager          |       |
| BMCManager          |       |
| OAM-LB Navigator    |       |
| BFSManager          |       |

### 3. 回避策

調査済の装置やシステムにおいて、非該当の場合には不要です。

ANRC シリーズは、全てのバージョンで該当するバージョンの Apache Tomcat を使用していますが、該当条件となる「デフォルトサーブレットの書き込みが有効」が無効になっているため条件が成立せず、脆弱性の影響はございません。将来的な予防措置として、次のリリースのタイミングにおいて Apache Tomcat のバージョン更新を検討してまいります。

AN-ManagerStation : 1.22.01 (2025/6/30 予定)

AN-Tracker : 2.10.01 (時期調整中)

A3CloudCNM は、該当条件となる「デフォルトサーブレットの書き込みが有効」が無効になっているため条件が成立せず、脆弱性の影響はございません。

### 4. 改訂履歴

2025/4/14 初版

2025/5/8 表 1 に調査の最新情報を反映

以上