

## OpenSSL の BN\_mod\_sqrt() における法が非素数のときに 無限ループを引き起こす問題 (JVNVU#90813125)

### 1. 脆弱性の概要

OpenSSL の BN\_mod\_sqrt() には、法が非素数の場合、無限ループを引き起こす問題があります。

- (1) 不正な楕円曲線パラメータを含む証明書や秘密鍵などをパースすることで無限ループを引き起こされ、サービス運用妨害 (DoS) 状態にな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	該当、対策されたファームウェアをお使いください。3. 回避策を参照
Apresia2000, 3000, 4000, 5000, 13000 シリーズ	AEOS7, AEOS6	該当
ApresiaNP7000 シリーズ	AEOS-NP7000	非該当
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 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	
XLGMC シリーズ	-	
XGMC シリーズ	-	
GMC シリーズ	-	
BMC シリーズ	-	
ApresiaAERO-5GC-A	-	
ApresiaAERO-CDU100	-	
ApresiaAERO-RU100	-	
ApresiaAERO-UE100	-	

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	
HCL Manager Station	
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。

該当の場合には修正後のバージョンを適用くださるようお願いいたします。

修正バージョンのリリース状況は以下の通りです。

製品名	OS バージョン	リリース日程
Apresia13000, 15000 シリーズ	AEOS8.44.01	2022/9/22 リリース済
Apresia2000, 3000, 4000, 5000, 13000 シリーズ	AEOS7.46.01 予定	2023/3 予定
ApresiaAERO-UE100	調整中	2023/3 予定

4. 改訂履歴

2022/5/26 初版

2022/10/12 Apresia13000, 15000 シリーズ、ApresiaAERO-UE100 対応状況更新