TD61-7990A
HCVU000000036
2022 年 11 月 15 日
APRESIA Systems 株式会社

OpenSSL に複数の脆弱性
(JVNVU#96381485)

1. 脆弱性の概要

OpenSSL には、次の脆弱性が存在します。

(1) RSA 秘密鍵の操作におけるヒープメモリ破損 - CVE-2022-2274

OpenSSL 3.0.4 リリースの AVX512IFMA 命令をサポートする X86_64CPU の RSA 実装不備により、2048 ビットの秘密鍵を使用すると、計算中にメモリ破壊が発生する

(2) AES OCB が一部のバイトの暗号化に失敗 - CVE-2022-2097

32 ビット x86 プラットフォーム向けの AES OCB モードにおいて、AES-NI アセンブリ最適化実装を使用するとデータが暗号化されない場合がある

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	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	-	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	
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
ApresiaAERO-UE100	調整中	調整中

4. 改訂履歴

2022/8/3　初版
2022/11/15　A　　表 2 に調査の最新情報を反映

以上