TD61-8032
HCVU000000039
2022 年 11 月 25 日
APRESIA Systems 株式会社

OpenSSL の NID_undef を使用したカスタム暗号における NULL 暗号化の脆弱性(JVNVU#92530096)

1. 脆弱性の概要

OpenSSL には、次の脆弱性が存在します。

(1) カスタム暗号作成をサポートする EVP_CIPHER_meth_new()関数および関連する関数にて、カスタム暗号を誤って処理することに起因し NULL 暗号化が発生すると、暗号文として平文が出力される

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	
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。

4. 改訂履歴

2022/11/25 初版

以上