TD61-7502B
HCVU000000025
2021 年 10 月 8 日
APRESIA Systems 株式会社

OpenSSL に複数の脆弱性(JVNVU#94508446, JVNVU#92126369)

1. 脆弱性の概要

OpenSSL には複数の脆弱性が存在します。

-- JVNVU#94508446 --

(1) 不正なフィールドを持つ X.509 証明書の検証処理を行うことで、サービス運用妨害(DoS)状態にされる (CVE-2021-23841)

(2) EVP_CipherUpdate、EVP_EncryptUpdate、EVP_DecryptUpdate 関数の呼び出し時にプラットフォーム上の整数の最大値に近い値を入力されることで、アプリケーションが不正な動作をしたり、クラッシュさせられたりする (CVE-2021-23840)

(3) RSA 署名に付与されるパディングの処理に起因するバージョンロールバック攻撃により攻撃者によって SSLv2 接続を強制される (CVE-2021-23839)

-- JVNVU#92126369 --

(4) SSL/TLS ハンドシェイクの再ネゴシエーション処理における NULL ポインタ参照 (CWE-476, CVE-2021-3449)

(5) X509_V_FLAG_X509_STRICT フラグ設定時の CA 証明書検証不備 (CWE-295, CVE-2021-3450)

2. 当社製品への影響

当社製品の本脆弱性に関する影響は下記の通りです。

表 1 ネットワーク装置

製品名	OS 名称	影響の有無
Apresia26000 シリーズ	AMIOS6	本脆弱性に該当しません。
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	

製品名	OS 名称	影響の有無
ApresiaLight FM シリーズ	APLFMOS	本脆弱性に該当しません。
ApresiaLight GM シリーズ	APLGMOS	
ApresiaLight GS シリーズ	APLGSOS	
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	-	
ApreisaAERO-CDU100	-	
ApresiaAERO-RU100	-	
ApresiaAERO-UE100	-	

表 2 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	調査中
ANRC シリーズ	本脆弱性に該当しません。
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、該当しないので特に必要ありません。

4. 改訂履歴

2021/5/14 初版

2021/6/15 A　　表１、表 2 に調査の最新状況を反映。

2021/10/8 B　　NP3000 シリーズ、ローカル 5G 製品を追加。
表１に調査の最新状況を反映。

以上