

OpenSSL に複数の脆弱性(JVNVU#99612123)

1. 脆弱性の概要

OpenSSL には以下に示す複数の脆弱性が存在します。

- (1) SM2 暗号データの復号処理におけるバッファオーバーフロー (CVE-2021-3711)
問題を引き起こす SM2 データがアプリケーションに渡されることで、アプリケーションの動作を変えられたり、クラッシュさせられたりする
- (2) ASN.1 文字列処理におけるバッファエラー (CVE-2021-3712)
影響を受ける関数に NULL 終端を持たない ASN1_STRING 構造を処理させられることにより、アプリケーションがクラッシュさせられたり、メモリ内のデータが読み取られたりする

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	CVE-2021-3712 に該当、2023 年 3 月までに修正予定
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	非該当
ApresiaLight GM シリーズ	APLGMOS	
ApresiaLight GM200 シリーズ	APLGM200OS	CVE-2021-3712 に該当、2023 年 6 月までに修正予定
ApresiaLight GS シリーズ	APLGSOS	CVE-2021-3712 該当、1.02.01 で修正済み

表2 ネットワーク装置2

製品名	OS 名称	影響の有無
APLMC シリーズ	APLMCOS	非該当
XLGMC シリーズ	-	
XGMC シリーズ	-	
GMC シリーズ	-	
BMC シリーズ	-	
ApresiaAERO-5GC-A	-	非該当
ApresiaAERO-CDU100	-	
ApresiaAERO-RU100	-	
ApresiaAERO-UE100	-	該当、次期 OS で修正予定

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。
 該当の場合には回避策はありません。修正後の OS を適用くださるようお願いします。

4. 改訂履歴

2021/10/8 初版

- 2022/3/31 A
- ・表 1、表 2、表 3 に調査の最新情報を反映
 - ・表 1 に ApresiaLight GM200 シリーズを追加
 - ・表 1、表 2、表 3 の反映内容に合わせ、3.回避策の内容を更新

以上