

OpenSSL の ChangeCipherSpec 処理の脆弱性 (VU#978508)

1. 脆弱性の概要

OpenSSL Project が提供する SSL/TLS ハンドシェイクにおける ChangeCipherSpec メッセージの処理に脆弱性が存在します。

2. 参考情報

OpenSSL における Change Cipher Spec メッセージの処理に脆弱性
<http://jvn.jp/jp/JVN61247051/index.html>

3. 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
Apresia26000 シリーズ	AMIOS6	本脆弱性に該当しません。
Apresia18000 シリーズ	AMIOS2	
Apresia16000 シリーズ	AMIOS3	
Apresia12000 シリーズ	AMIOS5	
Apresia8000 シリーズ	ApWare	
Apresia6000 シリーズ	ApbWare	
Apresia13000, 15000 シリーズ	AEOS8	
Apresia3000, 4000, 5000, 13000 シリーズ	AEOS7, AEOS6	
ApresiaLight FM シリーズ	APLFMOS	
ApresiaLight GM シリーズ	APLGMOS	
ApresiaLight シリーズ	APL-Ware	
XLGMC シリーズ	-	
XGMC シリーズ	-	
GMC シリーズ	-	
GMX シリーズ	-	
eWAVE シリーズ	-	
BMC シリーズ	-	
GMA シリーズ	-	

表2 ネットワーク管理システム

ソフトウェア名	影響
HCL Manager Station	本脆弱性に該当しません。
ApresiaManager	
MMRPManager	
Command Navigator	
ApresiaManager/C	
GMXManager	
GMAManager	
BMCManager	
OSWManager	
OAM-LB Navigator	
BFSManager	

4. 回避策

特に必要ありません。

以上