TD61-6072
HCVU000000021
2015 年 6 月 10 日
日立金属株式会社
電線材料カンパニー
情報システム統括部

TLS プロトコルにおける暗号アルゴリズムダウングレードの脆弱性 (JVNDB-2015-002764)

1. 脆弱性の概要

TLS プロトコルには、DHE_EXPORT 暗号※がサーバにおいて有効であり、かつクライアントにおいて無効である場合、強度の低い暗号アルゴリズムへのダウングレードが可能となる脆弱性があります。(CVE-2015-4000)

※Diffie-Hellman key Exchange 輸出グレード暗号

2. 参考情報

TLS プロトコルにおける暗号アルゴリズムのダウングレード攻撃を実行される脆弱性
http://jvndb.jvn.jp/ja/contents/2015/JVNDB-2015-002764.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	
Apresia2000,3000,4000, 5000,13000 シリーズ	AEOS7,AEOS6	
ApresiaLight FM シリーズ	APLFMOS	
ApresiaLight GM シリーズ	APLGMOS	
ApresiaLightGM152	APLGM152OS	
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