TD61-5971C
HCVU000000019
2015 年 6 月 30 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

OpenSSL の複数の脆弱性(JVNVU#98974537)

1. 脆弱性の概要

OpenSSL には複数の脆弱性が存在します。

(1) DTLS (Datagram TLS)を使用した攻撃に対し、サービス停止に至る可能性がある脆弱性 (CVE-2014-3571, CVE-2015-0206)

(2) DoS 攻撃に対し、サービス停止に至る可能性がある脆弱性 (CVE-2014-3569)

(3) DoS 攻撃に対し、強度の低い暗号化や RSA キーを提供する可能性がある脆弱性 (CVE-2014-3572, CVE-2015-0204)

(4) 細工された DH 証明書により不正なクライアントを認証する脆弱性 (CVE-2015-0205)

(5) 攻撃に対し保護機構の迂回を可能とする脆弱性 (CVE-2014-3570, CVE-2014-8275)

2. 参考情報

OpenSSL に複数の脆弱性
http://jvn.jp/vu/JVNVU98974537/

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	本脆弱性に該当します。 (CVE-2014-8275, CVE-2015-0204)
Apresia2000,3000,4000, 5000,13000 シリーズ	AEOS7,AEOS6	
ApresiaLight FM シリーズ	APLFMOS	本脆弱性に該当します。 (CVE-2014-3570, CVE-2015-0204)
ApresiaLight GM シリーズ	APLGMOS	
ApresiaLightGM152	APLGM152OS	
ApresiaLight シリーズ	APL-Ware	本脆弱性に該当しません。
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	

脆弱性に該当する装置では、以下の影響があります。

CVE-2014-8275

不正な証明書を使用すると、なりすましを許可する可能性があります。

CVE-2015-0204

攻撃者が装置と端末間の通信に介入すると強度の低い暗号に変更される可能性があります。

CVE-2014-3570

乱数生成の演算に問題があり、暗号が解読されやすくなる可能性があります。

4. 回避策

(1) AEOS7,AEOS8 で動作する装置は下記の修正済バージョンを適用ください。

本脆弱性に対し修正されたバージョンを下記に示します。

製品名(OS 名)	修正されたバージョン
Apresia3000,5000,13000(AEOS7)	7.38.01
Apresia13000,15000(AEOS8)	8.28.01

AEOS6 以前の修正バージョンのリリース予定はありません。

(2) APLFMOS,APLGMOS,APLGM152OS で動作する装置は下記の修正済バージョンを適用ください。

本脆弱性に対し修正されたバージョンを下記に示します。

製品名(OS 名)	修正されたバージョン
ApresiaLightFM(APLFMOS)	1.10.01
ApresiaLightGM(APLGMOS)	1.07.00
ApresiaLightGM152(APLGM152OS)	1.01.00

(3) 修正済バージョンを適用できない場合、不正な証明書を使用しない、あるいは装置と端末間の通信への介入を防ぐなどの対策により問題を回避することができます。

以上