TD61-5918D
HCVU000000017
2016 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

SSLv3 CBC モード利用時の脆弱性(CVE-2014-3566)

1. 脆弱性の概要

SSLv3 (version 3.0) には、中間者攻撃により SSL 通信の暗号文の解読を許してしまう脆弱性が存在します。SSLv3 でブロック暗号の CBC モード※による暗号化が行われている通信に対し、通信内容の解読を許してしまう可能性があります。

※ CBC: Cipher Block Chaining

2. 参考情報

SSLv3 プロトコルに暗号化データを解読される脆弱性(POODLE 攻撃)
http://jvn.jp/vu/JVNVU98283300/

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。
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	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	

Apresia13000, 15000 シリーズ (AEOS8)、Apresia2000, 3000, 4000, 5000, 13000 シリーズ (AEOS7,AEOS6) において AccessDefender あるいは NA (Network Authentication)機能の Web 認証(https)を使用しない場合は影響ありません。

ApresiaLight FM シリーズ (APLFMOS)、ApresiaLight GM シリーズ (APLGMOS)、ApresiaLightGM152(APLGM152OS)において、Web 認証(https)あるいは Web ベース GUI(https)を使用しない場合は影響ありません。

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)	7.36.01
Apresia13000,15000(AEOS8)	8.25.01

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)	1.10.00
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、クライアント側で SSLv3 を無効にすることにより問題を回避可能です。

以上