TD61-5968A
HCVU000000018
2015 年 1 月 16 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

ntpd の複数の脆弱性(JVNVU#96605606)

1．脆弱性の概要

Network Time Protocol (NTP)は、時刻同期のための通信プロトコルです。NTP を用いて装置間の時刻を同期する ntpd プログラムには複数の脆弱性が存在します。

(1) 擬似乱数生成器 (PRNG:Pseudo Random Number Generator)に起因して強度の低い暗号の使用を許してしまう脆弱性 (CVE-2014-9293、CVE-2014-9294)

(2) スタックバッファオーバーフローに起因して任意のコード実行を許してしまう脆弱性 (CVE-2014-9295)

(3) 特定のエラー発生時に処理が停止しない問題 (CVE-2014-9296)

2．参考情報

Network Time Protocol daemon (ntpd) に複数の脆弱性
https://jvn.jp/vu/JVNVU96605606/

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	
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

対応の必要はありません。

以上