TD61-5787
HCVU000000013
2014 年 6 月 13 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

OSPF LSA に関する脆弱性(VU#229804)

1. 脆弱性の概要

OSPF プロトコルには Link State Advertisement (LSA)の識別に関する問題があります。結果として、第三者が細工した LSA パケットを送信することで、ルーティングテーブルが改ざんされる可能性があります。

2. 参考情報

OSPF プロトコルの Link State Advertisement (LSA)に関する問題
http://www.jpcert.or.jp/wr/2013/wr133101.html#1

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。
Apresia3000,5000,13000 シリーズ	AEOS7, AEOS6	
Apresia4000 シリーズ	AEOS7, AEOS6	本脆弱性に該当しません。
ApresiaLight シリーズ	APL-Ware	
ApresiaLight FM シリーズ	APLFMOS	
ApresiaLight GM シリーズ	APLGMOS	
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	

AEOS6,AEOS7,AEOS8 で動作する Apresia3000,5000,13000,15000 シリーズにおいて、改ざんされた OSFP LSA を受信すると不正な LSA にも関わらず経路を学習する問題があります。

但し、OSPF LSA はルータの異なるセグメントを超えて転送されることはないため、セグメント(サブネット)外からの不正な OSPF LSA パケットにより影響を受ける可能性は極めて低いと考えられます。

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)	7.32.01
Apresia13000,15000(AEOS8)	8.21.01

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) OSPF 認証機能を有効にして、信頼されたルータ以外からの LSA を受け取らないようにしてください。完全に回避することはできませんが不正な操作を行うことがより困難となります。

5. 謝辞

本脆弱性情報についてご報告頂いた Gabi Nakibly 氏に深く感謝します。

以上