TD61-5790
HCVU000000013
Jun 13, 2014
Information Systems Products Business Unit
Cable Materials Company
Hitachi Metals, Ltd.

OSPF LSA Vulnerability (VU#229804)

1. Overview

The Open Shortest Path First (OSPF) protocol does not specify unique Link State Advertisement (LSA) lookup identifiers, which allow an attacker to intercept traffic or conduct a Denial of Service (DoS) attack.

2. References

Open Shortest Path First (OSPF) Protocol does not specify unique LSA lookup identifiers
http://www.kb.cert.org/vuls/id/229804

3. Impact

List the status of our products as following table.

Table-1 Network Equipment

Model	OS	Status
Apresia26000 Series	AMIOS6	Not Affected
Apresia18000 Series	AMIOS2	
Apresia16000 Series	AMIOS3	
Apresia12000 Series	AMIOS5	
Apresia8000 Series	ApWare	
Apresia6000 Series	ApbWare	
Apresia13000,15000 Series	AEOS8	Affected
Apresia3000,5000,13000 Series	AEOS7, AEOS6	
Apresia4000 Series	AEOS7, AEOS6	Not Affected
ApresiaLight Series	APL-Ware	
ApresiaLight FM Series	APLFMOS	
ApresiaLight GM Series	APLGMOS	
XLGMC Series	-	
XGMC Series	-	
GMC Series	-	
GMX Series	-	
eWAVE Series	-	
BMC Series	-	
GMA Series	-	

Table-2 Network Management System

Software	Status
HCL Manager Station	Not Affected
ApresiaManager	
MMRPManager	
Command Navigator	
ApresiaManager/C	
GMXManager	
GMAManager	
BMCManager	
OSWManager	
OAM-LB Navigator	
BFSManager	

Apresia3000, 4000, 5000, 13000, 15000 series may be affected by this vulnerability issue.
Receiving crafted OSPF LSA may cause falsification of their routing table.
To exploit this vulnerability, it may require access to trusted, internal networks to send crafted OSPF LSA.

4. Solution

(1) Software Upgrade

Software updates for AEOS7 and AEOS8 have been released to resolve this issue.
Release versions containing the fix are listed below.

Model (OS)	Version
Apresia3000, 5000, 13000 (AEOS7)	7.32.01 or later
Apresia13000, 15000 (AEOS8)	8.21.01 or later

(2) Enable OSPF authentication

Although this is not considered completely secure, it makes more difficult to attack.

5. Acknowledgement

Thanks to Dr. Gabi Nakibly for reporting this vulnerability.