

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans AirPort Extreme Base Station et Time Capsule

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-620>

Gestion du document

Référence	CERTA-2010-AVI-620
Titre	Vulnérabilités dans AirPort Extreme Base Station et Time Capsule
Date de la première version	17 décembre 2010
Date de la dernière version	–
Source(s)	
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Déni de service à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- Time Capsule, versions du micrologiciel inférieures à 7.5.2 ;
- AirPort Extreme Base Station, versions du micrologiciel inférieures à 7.5.2 ;

3 Résumé

De multiples vulnérabilités affectant le micrologiciel des appareils *Time Capsule* et *AirPort Extreme Base Station* permettent à un attaquant de contourner la politique de sécurité ou d'effectuer un déni de service à distance.

4 Description

Cinq vulnérabilités spécifiées par les références CVE suivantes ont été corrigées:

- un débordement d'entier dans la gestion du protocole SNMP permet à un attaquant de provoquer l'arrêt inopiné du service SNMP (CVE-2008-4390) ;

- un utilisateur malveillant du réseau peut effectuer un déni de service (redémarrage de la borne) en envoyant un grand nombre de paquets `IPv6`, ce qui consomme les ressources de l'appareil. (CVE-2009-2189);
- un attaquant peut contourner les règles de pare-feu et contacter un serveur FTP situé derrière le NAT (CVE-2010-0039);
- une erreur dans la gestion des paquets `ISAKMP` fragmentés par le démon `racoon` permet à un attaquant d'arrêter ce démon de manière inopinée (CVE-2010-1574);
- les appareils configurés pour fonctionner en mode pont (bridge), ou configurés en mode NAT avec un hôte par défaut subissent un déni de service lorsque des réponses `DHCP` spécialement conçues leur sont envoyés.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Apple APPLE-SA-2010-12-16-1 du 16 décembre 2010 :
<http://lists.apple.com/archives/security-announce/2010/Dec/msg00001.html>
- Référence CVE CVE-2008-4309 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4309>
- Référence CVE CVE-2009-2189 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2189>
- Référence CVE CVE-2009-1574 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1574>
- Référence CVE CVE-2010-0039 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0039>
- Référence CVE CVE-2010-1804 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1804>

Gestion détaillée du document

17 décembre 2010 version initiale.