

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans les produits Cisco Wireless LAN

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-422>

Gestion du document

Référence	CERTA-2010-AVI-422
Titre	Multiples vulnérabilités dans les produits Cisco Wireless LAN
Date de la première version	09 septembre 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité cisco-sa-20100908-wlc du 08 septembre 2010
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

- Dénis de service à distance ;
- contournement de la politique de sécurité ;
- élévation de privilèges.

2 Systèmes affectés

Les produits suivants sont affectés par ces vulnérabilités :

- Cisco Wireless LAN Controller série 2000 ;
- Cisco Wireless LAN Controller série 2100 ;
- Cisco Wireless LAN Controller série 4100 ;
- Cisco Wireless LAN Controller série 4400 ;
- Cisco Wireless LAN Controller série 5500 ;
- Cisco Wireless Services Modules ;
- Cisco Wireless LAN Controller Modules pour Integrated Services Routers ;
- Cisco Catalyst 3750G Integrated Wireless LAN Controller.

3 Résumé

De multiples vulnérabilités affectent la famille des produits *Cisco Wireless LAN Controller*, nommés ci-après *WLC*.

4 Description

Plusieurs types de vulnérabilités ont été découvertes :

- Un paquet *Internet Key Exchange* forgé par un attaquant à destination d'un *WLC Cisco* peut provoquer un déni de service. Ce protocole est activé par défaut sur ces produits et ne peut pas être désactivé. Les versions 3.2 et supérieures du logiciel sont affectées (cf. CVE-2010-0574).
- Un attaquant authentifié peut créer une série de paquets *HTTP* pour obliger l'appareil à redémarrer. La répétition de cette attaque provoque un déni de service (cf. CVE-2010-2841). Les versions 4.2 et supérieures des logiciels sont affectées.
- Il est possible à un attaquant authentifié sur l'appareil de contourner ses droits en lecture seule afin de modifier la configuration (cf. CVE-2010-2842, CVE-2010-2843 et CVE-2010-3033).
- Un attaquant non authentifié peut contourner certaines listes de contrôle d'accès à travers deux vulnérabilités (cf. CVE-2010-0575 et CVE-2010-3034). Une des deux vulnérabilités affecte les versions 4.1 et suivantes, l'autre les versions 6.0.x.

5 Solution

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

6 Documentation

- Bulletin de sécurité Cisco cisco-sa-20100908-wlc du 08 septembre 2010:
<http://cisco.com/warp/public/707/cisco-sa-20100908-wlc.shtml>
- Référence CVE CVE-2010-0574 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0574>
- Référence CVE CVE-2010-0575 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0575>
- Référence CVE CVE-2010-2841 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2841>
- Référence CVE CVE-2010-2842 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2842>
- Référence CVE CVE-2010-2843 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3124>
- Référence CVE CVE-2010-3033 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3033>
- Référence CVE CVE-2010-3034 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3034>

Gestion détaillée du document

09 septembre 2010 version initiale.