

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans Cisco Adaptive Security Appliances

---

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-2011-AVI-574>

---

### Gestion du document

Référence	CERTA-2011-AVI-574
Titre	Multiples vulnérabilités dans Cisco Adaptive Security Appliances
Date de la première version	18 octobre 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco 20111005-asa du 05 octobre 2011
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

- équipements Cisco série 5500 Adaptive Security Appliances ;
- équipements Cisco Catalyst série 6500 ASA Service Module.

## 3 Résumé

Plusieurs vulnérabilités permettant à un attaquant distant, soit de forcer l'équipement Cisco vulnérable à redémarrer, soit de contourner des politiques de sécurité ont été corrigées.

## 4 Description

Une première vulnérabilité dans le système d'inspection de paquets du protocole MSN IM permet à un attaquant de réaliser un déni de service lorsque celui-ci dirige du trafic spécialement conçu au travers de l'équipement vulnérable. L'équipement doit avoir activé l'inspection des paquets MSN IM (CVE-2011-3304).

Une vulnérabilité dans l'implémentation du protocole TACACS+ (*Terminal Access Controller Access-Control System Plus*) permet à un attaquant distant de contourner les règles de contrôle d'accès gérées par ce protocole (CVE-2011-3298).

Quatre vulnérabilités dans le système d'inspection des paquets du protocole SunRPC permettent à une personne malintentionnée de provoquer l'arrêt de l'appareil à distance au moyen de messages spécialement construits (CVE-2011-3299, CVE-2011-3300, CVE-2011-3301 et CVE-2011-3302).

Enfin, une vulnérabilité dans le système d'inspection de paquets du protocole ILS permet à un attaquant de réaliser un déni de service lorsque celui-ci dirige du trafic spécialement conçu au travers de l'équipement vulnérable. L'équipement doit avoir activé l'inspection des paquets ILS (CVE-2011-3303).

## 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 20111005-asa du 18 octobre 2011 :  
<http://www.cisco.com/warp/public/707/cisco-sa-20111005-asa.shtml>
- Référence CVE CVE-2011-3298 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3298>
- Référence CVE CVE-2011-3299 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3299>
- Référence CVE CVE-2011-3300 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3300>
- Référence CVE CVE-2011-3301 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3301>
- Référence CVE CVE-2011-3302 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3302>
- Référence CVE CVE-2011-3303 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3303>
- Référence CVE CVE-2011-3304 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3304>

## Gestion détaillée du document

**18 octobre 2011** version initiale.