

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités des produits Cisco

---

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-2009-AVI-134>

---

### Gestion du document

Référence	CERTA-2009-AVI-134
Titre	Vulnérabilités des produits Cisco
Date de la première version	10 avril 2009
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

- Cisco PIX 7.x et 8.x ;
- Cisco ASA 7.x et 8.x.

## 3 Résumé

Plusieurs vulnérabilités affectent les produits Cisco. Leurs exploitation permet de contourner la politique de sécurité ou de réaliser un déni de service à distance.

## 4 Description

Plusieurs vulnérabilités affectent les produits Cisco :

- lorsque la fonctionnalité *override account* est activée, une vulnérabilité permet de contourner l'authentification ;

- lorsqu'un boîtier Cisco ASA est serveur de VPN SSL ou lorsque l'interface de gestion ASDM est active, une vulnérabilité dans le traitement des paquets SSL et HTTP permet à un utilisateur malveillant de provoquer un rechargement de l'équipement ;
- un défaut de la gestion de la mémoire est présent dans le traitement des paquets TCP. Il est exploitable pour provoquer un déni de service dès lors qu'un service basé sur TCP est actif sur l'équipement (VPN SSL, ASDM, SSH...);
- le traitement défectueux des paquets H.323 permet à un utilisateur malveillant de provoquer le rechargement de l'équipement ;
- le traitement défectueux des paquets SQL\*Net permet à un utilisateur malveillant de provoquer le rechargement de l'équipement ;
- une erreur non précisée permet de ne pas tenir compte de l'interdiction d'accès implicite lors du traitement des listes de contrôle d'accès.

## 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 20090408-asa du 08 avril 2009 :  
<http://www.cisco.com/warp/public/707/cisco-sa-20090408-asa.shtml>
- Référence CVE CVE-2009-1155 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1155>
- Référence CVE CVE-2009-1156 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1156>
- Référence CVE CVE-2009-1157 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1157>
- Référence CVE CVE-2009-1158 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1158>
- Référence CVE CVE-2009-1159 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1159>
- Référence CVE CVE-2009-1160 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1160>

## Gestion détaillée du document

10 avril 2009 version initiale.