

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans les 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-2008-AVI-310>

---

### Gestion du document

Référence	CERTA-2008-AVI-310
Titre	Vulnérabilité dans les produits CISCO
Date de la première version	11 juin 2008
Date de la dernière version	–
Source(s)	Avis cisco-sa-20080610-snmpv3
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

Contournement de la politique de sécurité.

## 2 Systèmes affectés

- Cisco Application Control Engine Appliance ;
- Cisco Application Control Engine XML Gateway ;
- Cisco CATOS 6.x, 7.x, 8.x ;
- Cisco IOS 12.x, R12.x, XR 3.x ;
- Cisco NX-OS 4.x ;
- Cisco SAN-OS 2.x, 3.x (MDS 9000).

## 3 Résumé

Une vulnérabilité affectant des produits Cisco permet à une personne malintentionnée de contourner la politique de sécurité.

## 4 Description

La vulnérabilité détaillée dans l'avis CERTA-2008-AVI-302 du 10 juin 2008 affecte également certains produits Cisco. Ainsi, une personne malveillante peut usurper des paquets en envoyant des messages d'authentification HMAC spécialement construits.

## 5 Solution

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

## 6 Documentation

- Document du CERTA CERTA-2008-AVI-302 du 10 juin 2008 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-302/index.html>
- Bulletin de sécurité Cisco 20080610-snmpv3 du 10 juin 2008 :  
<http://www.cisco.com/warp/public/707/cisco-sa-20080610-snmpv3.shtml>
- Référence CVE CVE-2008-0960 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0960>

## Gestion détaillée du document

**11 juin 2008** version initiale.