

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans Cisco Security Manager

---

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-028>

---

### Gestion du document

Référence	CERTA-2009-AVI-028
Titre	Vulnérabilité dans Cisco Security Manager
Date de la première version	22 janvier 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20090121-csm du 21 janvier 2009
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

- Accès à distance à un service ;
- contournement de la politique de sécurité ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

- *Cisco Security Manager* versions 3.1.x ;
- *Cisco Security Manager* versions 3.2.x antérieures à 3.2.2.

## 3 Résumé

Une vulnérabilité dans *Cisco Security Manager* permet d'accéder à distance au service *IPS Event Viewer*.

## 4 Description

*Cisco IPS Event Viewer* (IEV) est un service de *Cisco Security Manager* (CSM) qui permet de visualiser et gérer les alertes de sécurité de cinq capteurs maximum. L'accès à ce service permet de configurer les filtres, d'importer et d'exporter des journaux, etc.

IEV est installé par défaut dans *Cisco Security Manager* mais n'est pas automatiquement démarré. Lorsqu'IEV est démarré, de nombreux ports TCP sont ouverts à la fois sur le serveur et sur le client. Lorsque le client IEV arrête sa session, les ports TCP du client sont fermés, mais pas ceux du serveur. En se connectant directement à un des ports TCP serveur, un utilisateur malintentionné peut obtenir un accès administrateur au service IEV et à sa base de données.

## 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-20090121-csm du 21 janvier 2009 :  
<http://www.cisco.com/warp/public/707/cisco-sa-20090121-csm.shtml>
- Référence CVE CVE-2008-3820 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3820>

## Gestion détaillée du document

22 janvier 2009 version initiale.