

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans 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-2007-AVI-447>

---

### Gestion du document

Référence	CERTA-2007-AVI-447
Titre	Multiples vulnérabilités dans des produits Cisco
Date de la première version	19 octobre 2007
Date de la dernière version	–
Source(s)	Bulletins de sécurité de Cisco 97836, 98612, 98711 et 98833 du 17 octobre 2007
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 ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

- Les logiciels suivants nécessitent l'application du correctif ICM7.1(5)\_ES46 :
  - Cisco Unified Intelligent Contact Management Enterprise ;
  - Cisco Unified ICM Hosted ;
  - Cisco Unified Contact Center Enterprise ;
  - Cisco Unified Contact center Hosted ;
  - Cisco Unified CallManager ;
  - Cisco System Unified Contact Enterprise.
- Les boîtiers Cisco PIX et ASA, avec les versions logicielles 7.0, 7.1, 7.2 et 8.0 sont vulnérables et nécessitent l'installation du correctif ;

- Les logiciels Cisco Unified CallManager 5.0 and Communications Manager 5.1 sont vulnérables, et nécessitent l'installation de la version 6.0 ;
- Le module Cisco Firewall Services (version antérieure à la 3.2) est vulnérable et nécessite l'installation de la mise à jour.

### 3 Résumé

Plusieurs correctifs pour de multiples vulnérabilités touchant des produits Cisco ont été mis en ligne.

### 4 Description

Plusieurs vulnérabilités permettant entre autre des dénis de service et le contournement des politiques de sécurité sont corrigés dans les correctifs mis en ligne par Cisco.

### 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 ID 97836 du 17 octobre 2007 :  
<http://www.cisco.com/warp/public/707/cisco-sa-20071017-IPCC.shtml>
- Bulletin de sécurité Cisco ID 98612 du 17 octobre 2007 :  
<http://www.cisco.com/warp/public/707/cisco-sa-20071017-fwsm.shtml>
- Bulletin de sécurité Cisco ID 98711 du 17 octobre 2007 :  
<http://www.cisco.com/warp/public/707/cisco-sa-20071017-asa.shtml>
- Bulletin de sécurité Cisco ID 98833 du 17 octobre 2007 :  
<http://www.cisco.com/warp/public/707/cisco-sa-20071017-cucm.shtml>
- Référence CVE CVE-2007-5537 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5537>
- Référence CVE CVE-2007-5538 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5538>
- Référence CVE CVE-2007-5539 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5539>

## Gestion détaillée du document

19 octobre 2007 version initiale.