

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans Cisco IOS

---

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-026>

---

### Gestion du document

Référence	CERTA-2011-AVI-026
Titre	Vulnérabilités dans Cisco IOS
Date de la première version	20 janvier 2011
Date de la dernière version	–
Source(s)	Bulletin de version Cisco IOS 15.0(1)XA5 du 28 décembre 2010
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.

## 2 Systèmes affectés

Cisco IOS 15.0(1)XA.

## 3 Résumé

Plusieurs vulnérabilités dans le système d'exploitation Cisco IOS permettent à un utilisateur malveillant de provoquer un déni de service à distance ou de contourner la politique de sécurité.

## 4 Description

Un utilisateur malveillant peut :

- provoquer un déni de service à distance au moyen de communications IRC, de flux SIP, de changements de numéro unique (SNR) ou d'annonces de routeurs en IPv6 ;

- contourner la politique de sécurité en raison d'une erreur dans la gestion des clefs publiques.

## 5 Solution

La version Cisco IOS 15.0(1)XA5 remédie à ces problèmes.

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

## 6 Documentation

- Bulletin de version Cisco IOS 15.0(1)XA5 du 28 décembre 2010 :  
[http://www.cisco.com/en/US/docs/ios/15\\_0/15\\_0x/15\\_01\\_XA/rn800xa.pdf](http://www.cisco.com/en/US/docs/ios/15_0/15_0x/15_01_XA/rn800xa.pdf)
- Référence CVE CVE-2009-5038 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-5038>
- Référence CVE CVE-2009-5040 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-5040>
- Référence CVE CVE-2010-4671 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4671>
- Référence CVE CVE-2010-4683 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4683>
- Référence CVE CVE-2010-4685 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4685>
- Référence CVE CVE-2010-4686 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4686>

## Gestion détaillée du document

20 janvier 2011 version initiale.