

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples 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-2009-AVI-402>

Gestion du document

Référence	CERTA-2009-AVI-402
Titre	Multiples vulnérabilités dans Cisco IOS
Date de la première version	24 septembre 2009
Date de la dernière version	–
Source(s)	Bulletins de sécurité Cisco IOS du 23 septembre 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

- Déni de service à distance ;
- déni de service ;
- contournement de la politique de sécurité ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

Cisco IOS 12.

pour de plus amples informations, se référer aux bulletins de sécurité de l'éditeur (cf. section Documentation).

3 Résumé

De multiples vulnérabilités ont été découvertes dans le système *Cisco IOS*. L'exploitation de ces vulnérabilités permet de contourner la politique de sécurité, de porter atteinte à la confidentialité des données, ou de réaliser un déni de service à distance.

4 Description

Neuf vulnérabilités ont été découvertes dans le système *Cisco IOS*. Ces vulnérabilités touchent de nombreuses parties du système et, pour la plupart, permettent à un utilisateur malintentionné de réaliser un déni de service.

Pour le détail complet des vulnérabilités, se référer aux bulletins de sécurité de l'éditeur (cf. section Documentation).

5 Solution

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

6 Documentation

- Bulletin de sécurité Cisco 20090923-ntp du 23 septembre 2009 :
<http://www.cisco.com/warp/public/707/cisco-sa-20090923-ntp.shtml>
- Bulletin de sécurité Cisco 20090923-ios-fw du 23 septembre 2009 :
<http://www.cisco.com/warp/public/707/cisco-sa-20090923-ios-fw.shtml>
- Bulletin de sécurité Cisco 20090923-auth-proy du 23 septembre 2009 :
<http://www.cisco.com/warp/public/707/cisco-sa-20090923-auth-proy.shtml>
- Bulletin de sécurité Cisco 20090923-tls du 23 septembre 2009 :
<http://www.cisco.com/warp/public/707/cisco-sa-20090923-tls.shtml>
- Bulletin de sécurité Cisco 20090923-sip du 23 septembre 2009 :
<http://www.cisco.com/warp/public/707/cisco-sa-20090923-sip.shtml>
- Bulletin de sécurité Cisco 20090923-h323 du 23 septembre 2009 :
<http://www.cisco.com/warp/public/707/cisco-sa-20090923-h323.shtml>
- Bulletin de sécurité Cisco 20090923-acl du 23 septembre 2009 :
<http://www.cisco.com/warp/public/707/cisco-sa-20090923-acl.shtml>
- Bulletin de sécurité Cisco 20090923-tunnels du 23 septembre 2009 :
<http://www.cisco.com/warp/public/707/cisco-sa-20090923-tunnels.shtml>
- Bulletin de sécurité Cisco 20090923-ipsec du 23 septembre 2009 :
<http://www.cisco.com/warp/public/707/cisco-sa-20090923-ipsec.shtml>

Gestion détaillée du document

24 septembre 2009 version initiale.