



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité
des systèmes d'information
CERTA

Paris, le 26 mars 2010
N° CERTA-2010-AVI-136

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-2010-AVI-136>

Gestion du document

Référence	CERTA-2010-AVI-136
Titre	Multiples vulnérabilités dans Cisco IOS
Date de la première version	26 mars 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco 20100324-ipsec du 24 mars 2010 Bulletin de sécurité Cisco 20100324-scp du 24 mars 2010 Bulletin de sécurité Cisco 20100324-ldp du 24 mars 2010 Bulletin de sécurité Cisco 20100324-h323 du 24 mars 2010 Bulletin de sécurité Cisco 20100324-sip du 24 mars 2010 Bulletin de sécurité Cisco 20100324-tcp du 24 mars 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

- Exécution de code arbitraire à distance ;
- déni de service à distance.

2 Systèmes affectés

- Cisco IOS 12.x et 15.x ;
- Cisco IOS XE 2.x ;
- Cisco IOS XR 3.x.

Une liste plus détaillée des systèmes affectés est disponible dans les bulletins de sécurité de l'éditeur.

3 Résumé

De multiples vulnérabilités dans les systèmes Cisco IOS permettent de provoquer un déni de service à distance ou d'exécuter du code arbitraire à distance.

4 Description

De multiples vulnérabilités ont été découvertes dans les systèmes Cisco IOS :

- une erreur dans la gestion des flux réseaux servant à l'échange des clés cryptographiques peut être exploitée afin de provoquer un redémarrage de Cisco IOS ;
- un message SCCP (protocole propriétaire Skinny Call Control Protocol) spécialement conçu peut faire redémarrer Cisco IOS ;
- un paquet réseau LDP UDP (technologie liée aux réseaux MPLS) spécialement conçu peut faire redémarrer Cisco IOS ;
- deux vulnérabilités existent dans le code H. 323 de Cisco IOS, une exploitation réussie de ces vulnérabilités provoque un déni de service à distance ou une exécution de code arbitraire à distance ;
- plusieurs vulnérabilités ont été découvertes dans le code SIP de Cisco IOS, une exploitation réussie de ces vulnérabilités provoque un déni de service à distance ou une exécution de code arbitraire à distance ;
- un segment TCP spécialement conçu peut bloquer ou faire redémarrer Cisco IOS.

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 20100324-ipsec du 24 mars 2010 :
<http://www.cisco.com/warp/public/707/cisco-sa-20100324-ipsec.shtml>
- Bulletin de sécurité Cisco 20100324-sccp du 24 mars 2010 :
<http://www.cisco.com/warp/public/707/cisco-sa-20100324-sccp.shtml>
- Bulletin de sécurité Cisco 20100324-ldp du 24 mars 2010 :
<http://www.cisco.com/warp/public/707/cisco-sa-20100324-ldp.shtml>
- Bulletin de sécurité Cisco 20100324-h323 du 24 mars 2010 :
<http://www.cisco.com/warp/public/707/cisco-sa-20100324-h323.shtml>
- Bulletin de sécurité Cisco 20100324-sip du 24 mars 2010 :
<http://www.cisco.com/warp/public/707/cisco-sa-20100324-sip.shtml>
- Bulletin de sécurité Cisco 20100324-tcp du 24 mars 2010 :
<http://www.cisco.com/warp/public/707/cisco-sa-20100324-tcp.shtml>
- Référence CVE CVE-2010-0576 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0576>
- Référence CVE CVE-2010-0577 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0577>
- Référence CVE CVE-2010-0578 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0578>
- Référence CVE CVE-2010-0579 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0579>
- Référence CVE CVE-2010-0580 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0580>
- Référence CVE CVE-2010-0581 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0581>
- Référence CVE CVE-2010-0582 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0582>

- Référence CVE CVE-2010-0583 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0583>
- Référence CVE CVE-2010-0584 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0584>

Gestion détaillée du document

26 mars 2010 version initiale.