

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-118>

Gestion du document

Référence	CERTA-2009-AVI-118
Titre	Multiples vulnérabilités dans Cisco IOS
Date de la première version	26 mars 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco 20090325-bundle du 25 mars 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 ;
- contournement de la politique de sécurité ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

Cisco IOS 12.x.

3 Résumé

De multiples vulnérabilités ont été découvertes dans Cisco IOS et permettent notamment à une personne malintentionnée de provoquer un déni de service à distance ou de porter atteinte à la confidentialité et l'intégrité des données.

4 Description

Plusieurs vulnérabilités ont été découvertes dans Cisco IOS :

- plusieurs vulnérabilités permettent, via une série de paquets *TCP* spécialement construits, de provoquer un déni de service ou un redémarrage du périphérique notamment lorsque le périphérique est configuré comme un serveur *Easy VPN* avec une encapsulation *Cisco Tunneling Control Protocol (cTCP)* ;
- une séquence de paquets *TCP/IP* spécialement construits permet de provoquer les effets suivants :
 - plus de nouvelles connexions ou sessions acceptées ;
 - consommation de la mémoire du périphérique ;
 - consommation excessive et prolongée du *CPU* ;
 - redémarrage du périphérique.
- une erreur dans la gestion des fonctionnalités *Mobile IP Network Translation Traversal* et *Mobile IPv6* permet de provoquer un déni de service ;
- une vulnérabilité dans le serveur *Secure Copy (SCP)* de Cisco IOS permet à un utilisateur authentifié ayant accès à une invite de commande de contourner la politique de sécurité et porter atteinte à la confidentialité et l'intégrité des données ;
- une erreur dans le protocole *SIP (Session Initiation Protocol)* permet de provoquer un redémarrage du périphérique à distance ;
- une erreur dans la gestion de certaines fonctionnalités permet, via une série de paquets *UDP* spécialement construits, de provoquer un déni de service.
- deux vulnérabilités dans Cisco IOS WebVPN et Cisco IOS SSLVPN permettent à une personne mal-intentionnée de provoquer un déni de service.

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 20090325-bundle du 25 mars 2009 :
<http://www.cisco.com/warp/public/707/cisco-sa-20090325-bundle.shtml>
- Référence CVE CVE-2009-0626 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0626>
- Référence CVE CVE-2009-0628 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0628>
- Référence CVE CVE-2009-0629 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0629>
- Référence CVE CVE-2009-0630 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0630>
- Référence CVE CVE-2009-0631 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0631>
- Référence CVE CVE-2009-0633 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0633>
- Référence CVE CVE-2009-0634 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0634>
- Référence CVE CVE-2009-0635 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0635>
- Référence CVE CVE-2009-0636 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0636>
- Référence CVE CVE-2009-0637 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0637>

Gestion détaillée du document

26 mars 2009 version initiale.