

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-2008-AVI-474>

Gestion du document

Référence	CERTA-2008-AVI-474
Titre	Multiples vulnérabilités dans Cisco IOS
Date de la première version	25 septembre 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco #107631 du 24 septembre 2008
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 12.x et dérivés.

3 Résumé

Plusieurs vulnérabilités présentes dans les IOS Cisco permettent à un utilisateur distant malintentionné de provoquer un déni de service ou de contourner la politique de sécurité du système.

4 Description

Plusieurs vulnérabilités sont présentes dans le système d'exploitation IOS des équipements Cisco. Ces failles sont relatives à la mise en œuvre par l'IOS :

- de la couche SSL (Bulletin Cisco #107631) ;

- du *multicast* (Bulletin Cisco #107550);
- de la translation d'adresse : NAT (Bulletin Cisco #99866);
- du protocole SIP : Session Initiation Protocol (Bulletin Cisco #107617 et 107971);
- des fonctionnalités d'IPS : Intrusion Prevention System (Bulletin Cisco #107583);
- du protocole SNMP : Simple Network Management Protocol (Bulletin Cisco #107696);
- du MPLS : Multiprotocol Label Switching (Bulletin Cisco #107578 et 107646);
- du système d'IPC : Inter-Process Communication (Bulletin Cisco #107661);
- du firewall AIC : firewall Application Inspection Control (Bulletin Cisco #107716);
- et du protocole L2TP : Layer 2 Tunneling Protocol (Bulletin Cisco #107441).

La vulnérabilité relative aux VPN MPLS (Bulletin Cisco #107578) permet à un utilisateur distant malintentionné de contourner la politique de sécurité du système vulnérable. Toutes les autres vulnérabilités permettent à un utilisateur distant malintentionné de provoquer un déni de service.

5 Solution

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

6 Documentation

- Bulletins de sécurité Cisco du 24 septembre 2008 :
 - <http://www.cisco.com/warp/public/707/cisco-sa-20080924-bundle.shtml>
 - <http://www.cisco.com/warp/public/707/cisco-sa-20080924-iosips.shtml>
 - <http://www.cisco.com/warp/public/707/cisco-sa-20080924-ssl.shtml>
 - <http://www.cisco.com/warp/public/707/cisco-sa-20080924-sip.shtml>
 - <http://www.cisco.com/warp/public/707/cisco-sa-20080924-cucm.shtml>
 - <http://www.cisco.com/warp/public/707/cisco-sa-20080924-vpn.shtml>
 - <http://www.cisco.com/warp/public/707/cisco-sa-20080924-ipc.shtml>
 - <http://www.cisco.com/warp/public/707/cisco-sa-20080924-mfi.shtml>
 - <http://www.cisco.com/warp/public/707/cisco-sa-20080924-ubr.shtml>
 - <http://www.cisco.com/warp/public/707/cisco-sa-20080924-sccp.shtml>
 - <http://www.cisco.com/warp/public/707/cisco-sa-20080924-multicast.shtml>
 - <http://www.cisco.com/warp/public/707/cisco-sa-20080924-iosfw.shtml>
 - <http://www.cisco.com/warp/public/707/cisco-sa-20080924-l2tp.shtml>

Gestion détaillée du document

25 septembre 2008 version initiale.