

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-456>

Gestion du document

Référence	CERTA-2010-AVI-456
Titre	Multiples vulnérabilités dans Cisco IOS
Date de la première version	24 septembre 2010
Date de la dernière version	–
Source(s)	Bulletins de sécurités Cisco du 22 septembre 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

Déni de service à distance.

2 Systèmes affectés

Les équipements utilisant Cisco IOS comme système d'exploitation.

3 Résumé

Plusieurs vulnérabilités sont présentes dans Cisco IOS. Toutes ces vulnérabilités permettent à un utilisateur distant malintentionné de provoquer un déni de service.

4 Description

Plusieurs vulnérabilités sont présentes dans le système d'exploitation Cisco IOS utilisé sur les équipements Cisco (eg. routeurs, commutateurs, etc.). Elles sont relatives à la mise en œuvre :

- de la translation d'adresse (NAT) ;
- du protocole SIP ;

- des VPN de type SSL ;
- du protocole H323 ;
- du protocole IGMP.

Toutes ces failles permettent à un utilisateur malintentionné de provoquer un déni de service à distance si une ou plusieurs de ces fonctionnalités sont activées sur l'équipement vulnérable.

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 20100922-nat du 22 septembre 2010 :
<http://www.cisco.com/warp/public/707/cisco-sa-20100922-nat.shtml>
- Bulletin de sécurité Cisco 20100922-sip du 22 septembre 2010 :
<http://www.cisco.com/warp/public/707/cisco-sa-20100922-sip.shtml>
- Bulletin de sécurité Cisco 20100922-sslvpn du 22 septembre 2010 :
<http://www.cisco.com/warp/public/707/cisco-sa-20100922-sslvpn.shtml>
- Bulletin de sécurité Cisco 20100922-h323 du 22 septembre 2010 :
<http://www.cisco.com/warp/public/707/cisco-sa-20100922-h323.shtml>
- Bulletin de sécurité Cisco 20100922-igmp du 22 septembre 2010 :
<http://www.cisco.com/warp/public/707/cisco-sa-20100922-igmp.shtml>
- Référence CVE CVE-2010-2831 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2831>
- Référence CVE CVE-2010-2835 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2835>
- Référence CVE CVE-2009-2051 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2051>
- Référence CVE CVE-2010-2834 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2834>
- Référence CVE CVE-2010-2836 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2836>
- Référence CVE CVE-2010-2828 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2828>
- Référence CVE CVE-2010-2829 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2829>
- Référence CVE CVE-2010-2830 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2830>

Gestion détaillée du document

24 septembre 2010 version initiale.