

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Cisco ASA et ASASM

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-2012-AVI-150>

Gestion du document

Référence	CERTA-2012-AVI-150
Titre	Vulnérabilités dans Cisco 6500 et 5500
Date de la première version	16 mars 2012
Date de la dernière version	–
Source	Bulletin de sécurité Cisco 20120314-asa du 14 mars 2012
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

- Cisco 5500 Adaptive Security Appliance (ASA) ;
- Cisco Catalyst 6500 ASA Services Module.

Cisco PIX peut être affecté par certaines de ces vulnérabilités, mais ce produit n'est plus maintenu.

3 Résumé

Plusieurs vulnérabilités dans des produits Cisco permettent à un attaquant de provoquer un déni de service à distance.

4 Description

Plusieurs modules dans les produits Cisco ASA et ASASM contiennent des vulnérabilités :

- le moteur d’inspection du trafic UDP ;
- le moteur de recherche d’attaques (*Threat Detection*), non activé par défaut ;
- le client Syslog ;
- le gestionnaire du protocole PIM (voir l’avis CERTA-2012-AVI-149).

Ces vulnérabilités permettent à un attaquant de provoquer un déni de service à distance.

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 20120314-asa du 14 mars 2012 :
<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120314-asa>
- Document du CERTA CERTA-2012-AVI-149 du 16 mars 2012 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-149/index.html>
- Référence CVE CVE-2012-0353 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0353>
- Référence CVE CVE-2012-0354 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0354>
- Référence CVE CVE-2012-0355 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0355>
- Référence CVE CVE-2012-0356 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0356>

Gestion détaillée du document

16 mars 2012 version initiale.