Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 juin 2012
N° CERTA-2012-AVI-347

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Cisco ASA 5500 et Cisco Catalyst 6500

Gestion du document

Référence	CERTA-2012-AVI-347
Titre	Vulnérabilité dans Cisco ASA 5500 et Cisco Catalyst 6500
Date de la première version	21 juin 2012
Date de la dernière version	–
Source(s)	
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 ASA 5500 et Cisco Catalyst 6500 avec le module ASA Services (ASASM), versions:
- 8.4 inférieures à 8.4(4.1) ;
- 8.5 inférieures à 8.5(1.11) ;
- 8.6 inférieures à 8.6(1.3).

3 Résumé

Une vulnérabilité a été corrigée dans ces produits Cisco. Celle-ci permet à un attaquant distant de forcer le rédémarrage de l'équipement au moyen de paquets IPv6 spécialement conçus.

4 Solution

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

5 Documentation

- Bulletin de sécurité Cisco 20120620-asaipv6 du 20 juin 2012 :
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120620-asaipv6
- Référence CVE CVE-2012-3058 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3058

Gestion détaillée du document

21 juin 2012 version initiale.