

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Cisco ASA série 5500

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-2011-AVI-109>

Gestion du document

Référence	CERTA-2011-AVI-109
Titre	Multiples vulnérabilités dans Cisco ASA série 5500
Date de la première version	24 février 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20110223-asa du 23 février 2011
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 ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

Cisco ASA Adaptive Security Appliances série 5500, dans les versions qui suivent. Vulnérabilité « pare-feu transparent » (CVE-2011-0393) :

- versions 7.0 strictement inférieures à 7.0(8.12) ;
- versions 7.1 ;
- versions 7.2 strictement inférieures à 7.2(5.2) ;
- versions 8.0 strictement inférieures à 8.0(5.21) ;
- versions 8.1 strictement inférieures à 8.1(2.49) ;
- versions 8.2 strictement inférieures à 8.2(3.6) ;
- versions 8.3 strictement inférieures à 8.3(2.7).

Vulnérabilité « SCCP » (CVE-2011-0394) :

- versions 7.0 strictement inférieures à 7.0(8.11) ;
- versions 7.1 ;

- versions 7.2 strictement inférieures à 7.2(5.1) ;
- versions 8.0 strictement inférieures à 8.0(5.19) ;
- versions 8.1 strictement inférieures à 8.1(2.47) ;
- versions 8.2 strictement inférieures à 8.2(2.19) ;
- versions 8.3 strictement inférieures à 8.3(1.8).

Vulnérabilité « *RIP* » (CVE-2011-0395) :

- versions 8.0 strictement inférieures à 8.0(5.20) ;
- versions 8.1 strictement inférieures à 8.1(2.48) ;
- versions 8.2 strictement inférieures à 8.2(3) ;
- versions 8.3 strictement inférieures à 8.3(2.1).

Vulnérabilité « accès non autorisé » (CVE-2011-0396) :

- versions 8.0 strictement inférieures à 8.0(5.23) ;
- versions 8.1 strictement inférieures à 8.1(2.49) ;
- versions 8.2 strictement inférieures à 8.2(4.1) ;
- versions 8.3 strictement inférieures à 8.3(2.13).

3 Résumé

Quatre vulnérabilités ont été corrigées dans les appareils Cisco ASA série 5500. Trois d’entre elles permettent de réaliser un déni de service à distance, et la quatrième permet d’accéder à des données confidentielles sur le système de fichiers.

4 Description

Une vulnérabilité concerne le pare-feu intégré si celui-ci est configuré en mode « transparent » (le mode par défaut est le mode « routé »). Un attaquant peut épuiser les ressources du système en envoyant des paquets IPv6 particuliers.

Une vulnérabilité dans le module d’inspection de trafic *SCCP* permet à un attaquant de forcer le rechargement de la configuration de l’équipement en envoyant un paquet spécialement conçu. Par défaut, cette fonction d’inspection de trafic est activée.

Lorsque le protocole *RIP* ainsi que la fonctionnalité Cisco Phone Proxy sont activés sur l’appareil, une personne malveillante peut forcer le redémarrage de celui-ci en envoyant des paquets *RIP* valides.

Enfin, lorsque l’équipement est configuré comme autorité locale de certification, un attaquant distant non authentifié peut exploiter une vulnérabilité pour accéder à des données confidentielles sur le système de fichiers.

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 cisco-sa-20110223-asa du 23 février 2011 :
<http://www.cisco.com/warp/public/707/cisco-sa-20110223-asa.shtml>
- Référence CVE CVE-2011-0393 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0393>
- Référence CVE CVE-2011-0394 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0394>
- Référence CVE CVE-2011-0395 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0395>
- Référence CVE CVE-2011-0396 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0396>

Gestion détaillée du document

24 février 2011 version initiale.