Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 juin 2010
N° CERTA-2010-AVI-292-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Cisco ASA

Gestion du document

Référence	CERTA-2010-AVI-292-001
Titre	Vulnérabilités dans Cisco ASA
Date de la première version	28 juin 2010
Date de la dernière version	30 juin 2010
Source(s)	Notes de version Cisco ASA version 8.1(2)
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 ;
- contournement de la politique de sécurité ;
- injection de code indirecte.

2 Systèmes affectés

Cisco ASA versions 8.1(1) et antérieures.

3 Résumé

De nombreuses vulnérabilités ont été trouvées dans Cisco ASA. Elles permettent de réaliser un déni de service à distance, de contourner la politique de sécurité ou de réaliser de l'injection de code indirecte.

4 Description

Plusieurs vulnérabilités sont présentes dans Cisco ASA. En particulier :

- deux vulnérabilités permettent à une personne malveillante d'injecter du code dans les réponses HTTP émises par le serveur et ainsi de faire exécuter du code dans le navigateur Web de la victime ;

- les gestions incorrectes des protocoles IPv6 et SSL permettent à un utilisateur malveillant de contourner la politique de sécurité ;
- un problème de traitement des certificats X.509 permet à un utilisateur malveillant d'épuiser la mémoire de l'équipement ;
- une vulnérabilité non précisée ainsi qu'un trafic SIP important permettent à un utilisateur malveillant distant de provoquer le redémarrage de l'équipement ;
- DTLS, IPsec L2L, les VPN SSL et des paquets TCP malformés sont utilisables par un attaquant pour 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

- Notes de version Cisco ASA version 8.1(2) :
  http://www.cisco.com/en/US/docs/security/asa/asa81/release/notes/asarn812.html
- Référence CVE CVE-2008-7257 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-7257
- Référence CVE CVE-2009-4910 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4910
- Référence CVE CVE-2009-4911 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4911
- Référence CVE CVE-2009-4912 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4912
- Référence CVE CVE-2009-4913 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4913
- Référence CVE CVE-2009-4914 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4914
- Référence CVE CVE-2009-4915 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4915
- Référence CVE CVE-2009-4916 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4916
- Référence CVE CVE-2009-4917 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4917
- Référence CVE CVE-2009-4918 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4918
- Référence CVE CVE-2009-4919 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4919
- Référence CVE CVE-2009-4920 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4920
- Référence CVE CVE-2009-4921 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4921
- Référence CVE CVE-2009-4922 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4922
- Référence CVE CVE-2009-4923 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4923

Gestion détaillée du document

28 juin 2010 version initiale.

30 juin 2010 ajout de vulnérabilités et de 14 références CVE.