Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 janvier 2011
N° CERTA-2011-AVI-025

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Cisco ASA

Gestion du document

Référence	CERTA-2011-AVI-025
Titre	Vulnérabilités dans Cisco ASA
Date de la première version	20 janvier 2011
Date de la dernière version	–
Source(s)	Bulletin de version Cisco 8.2 du 15 décembre 2010 Bulletin de version Cisco 8.3 du 02 août 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 ;
- contournement de la politique de sécurité.

2 Systèmes affectés

Cisco ASA 8.2(x) et 8.3(x).

3 Résumé

De nombreuses vulnérabilités affectent Cisco ASA et permettent à un utilisateur malveillant de contourner la politique de sécurité ou de provoquer un déni de service à distance.

4 Description

Des traitements défaillants du protocole Telnet, des paquets reçus lors de la mise en route, des requêtes CIFS par WebVPN et des requêtes HTTP par le service *Mobile User Security* permettent à un utilisateur malveillant de contourner des restrictions d'accès.

Des défauts dans les traitements des échecs de connexion OCSP et des protocoles EIGRP et LDAP permettent à un utilisateur malveillant d'épuiser les ressources.

Le traitement des trafics IPSec, SIP et de flux *multicast* non précisés ainsi que l'analyse de certains champs par emWEB permettent à un utilisateur malveillant de provoquer un arrêt inopiné du système.

Une erreur dans le traitement SMTP permet de contourner l'inspection des paquets.

5 Solution

Les versions 8.2(4) et 8.3(2) remédient à ces problèmes.

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

6 Documentation

- Bulletin de version Cisco 8.2 du 15 décembre 2010 :
  http://www.cisco.com/en/US/docs/security/asa/asa82/release/notes/asarn82.html
- Bulletin de version Cisco 8.3 du 02 août 2010 :
  http://www.cisco.com/en/US/docs/security/asa/asa83/release/notes/asarn83.html
- Référence CVE CVE-2010-4672 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4672
- Référence CVE CVE-2010-4675 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4675
- Référence CVE CVE-2010-4676 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4676
- Référence CVE CVE-2010-4677 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4677
- Référence CVE CVE-2010-4678 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4678
- Référence CVE CVE-2010-4679 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4679
- Référence CVE CVE-2010-4680 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4680
- Référence CVE CVE-2010-4681 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4681
- Référence CVE CVE-2010-4682 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4682
- Référence CVE CVE-2010-4688 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4688
- Référence CVE CVE-2010-4690 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4690
- Référence CVE CVE-2010-4691 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4691
- Référence CVE CVE-2010-4692 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4692

Gestion détaillée du document

20 janvier 2011 version initiale.