Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 18 février 2010
N° CERTA-2010-AVI-085

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de Cisco ASA

Gestion du document

Référence	CERTA-2010-AVI-085
Titre	Vulnérabilités de Cisco ASA
Date de la première version	18 février 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco 20100217-asa du 17 février 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 5500 series.

3 Résumé

Plusieurs vulnérabilités de Cisco ASA ont été publiées. Elles sont exploitables par un utilisateur malveillant pour provoquer un déni de service à distance ou pour contourner l'authentification.

4 Description

Plusieurs vulnérabilités de Cisco ASA ont été publiées :

- à la réception de certains segments (PDU) TCP lors de la phase de terminaison d'une connexion TCP, la création de nouvelle connexion peut devenir impossible. Cela permet à un utilisateur malveillant de provoquer un déni de service à distance par épuisement des ressources ;

- deux vulnérabilités dans le traitement des paquets SIP en transit permettent à un utilisateur malveillant de provoquer un redémarrage du boîtier Cisco ;
- une vulnérabilité dans le traitement des paquets SCCP en transit permet à un utilisateur malveillant de provoquer un redémarrage du boîtier Cisco ;
- une vulnérabilité dans le traitement de paquets DTLS malformés à destination du boîtier permet à un utilisateur malveillant de provoquer un redémarrage du boîtier Cisco. Le boîtier doit être configuré pour le transport DTLS et pour WebVPN ;
- une vulnérabilité dans le traitement de paquets TCP malformés en transit permet à un utilisateur malveillant, dans des conditions particulières, de provoquer un redémarrage du boîtier Cisco ;
- une vulnérabilité dans le traitement des messages IKE permet à un utilisateur de mettre fin à un tunnel IPsec ;
- une vulnérabilité affecte les boîtiers configurés pour authentifier des utilisateurs avec le protocole NTLMv1. Elle permet de contourner l'authentification.

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 20100217-asa du 17 février 2010 :
  http://www.cisco.com/warp/public/707/cisco-sa-20100217-asa.shtml
- Référence CVE CVE-2010-0149 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0149
- Référence CVE CVE-2010-0150 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0150
- Référence CVE CVE-2010-0151 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0151
- Référence CVE CVE-2010-0565 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0565
- Référence CVE CVE-2010-0566 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0566
- Référence CVE CVE-2010-0567 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0567
- Référence CVE CVE-2010-0568 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0568
- Référence CVE CVE-2010-0569 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0569

Gestion détaillée du document

18 février 2010 version initiale.