Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 03 mai 2007
N° CERTA-2007-AVI-198

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Cisco ASA et PIX

Gestion du document

Référence	CERTA-2007-AVI-198
Titre	Multiples vulnérabilités dans Cisco ASA et PIX
Date de la première version	03 mai 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco 82451 du 02 mai 2007
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 ;
- élévation de privilèges.

2 Systèmes affectés

- Cisco ASA (*Adaptive Security Appliance*), pour les versions logicielles 7.1 et 7.2 antérieures à 7.1(2)49 et 7.2(2)19 ;
- Cisco PIX, pour les versions logicielles 7.1 et 7.2 antérieures à 7.1(2)49 et 7.2(2)19.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans les produits Cisco ASA et PIX. L'exploitation de celles-ci permettent à un utilisateur distant de contourner la politique de sécurité, ou de perturber le fonctionnement du système vulnérable.

4 Description

Plusieurs vulnérabilités ont été identifiées dans les produits Cisco ASA et PIX. Parmi celles-ci :

- dans le contexte d'un tunnel L2TP, il serait possible de contourner le processus d'authentification LDAP, lorsque le protocole utilisé n'est pas PAP (*Password Authentication Protocol*), mais CHAP, MS-CHAPv1 ou MS-CHAPv2 par exemple ;
- la vulnérabilité précédente serait également applicable au cours de la phase d'authentification des sessions d'administration (telnet, SSH ou HTTP) ;
- la gestion de la date d'expiration des mots de passe ne serait pas correctement prise en compte au cours de la fermeture d'une connexion distante VPN IPSec ;
- une situation de compétition (ou *race condition*) existerait dans la manipulation de sessions SSL particulières par Cisco ASA. Cette vulnérabilité peut provoquer le redémarrage du système.
- DHCP est un protocole permettant de fournir automatiquement des éléments de configuration aux machines du réseau (adresse IP, masque de réseau, adresse de la passerelle par défaut, adresse du serveur DNS, etc.). ASA et PIX offrent la possibilité d'utiliser le système comme agent de liaison DHCP vers les serveurs DHCP du réseau. Les paquets de type DHCPREQUEST ou DHCPINFORM provoquent des réponses de la forme DHCPACK de la part des serveurs DHCP. Les agents de relais Cisco ne parviendraient pas à stocker toutes les informations concernant ces échanges, et bloqueraient des paquets. Cette vulnérabilité peut donc être utilisée par une personne malveillante pour empêcher l'agent de relais de transférer les paquets légitimes.

5 Solution

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

6 Documentation

- Bulletin de sécurité Cisco ID 82451 du 02 mai 2007 :
  http://www.cisco.com/warp/public/707/cisco-sa-20070502-asa.shtml
- Document de réponse Cisco ID 91337 du 02 mai 2007 :
  http://www.cisco.com/warp/public/707/cisco-sr-20070502-pix.shtml
- Référence CVE CVE-2007-2461 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2461
- Référence CVE CVE-2007-2462 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2462
- Référence CVE CVE-2007-2463 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2463
- Référence CVE CVE-2007-2464 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2464

Gestion détaillée du document

03 mai 2007 version initiale.