

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Plusieurs vulnérabilités dans Cisco PIX et ASAX

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-2008-AVI-287>

Gestion du document

Référence	CERTA-2008-AVI-287
Titre	Plusieurs vulnérabilités dans Cisco PIX et ASAX
Date de la première version	05 juin 2008
Date de la dernière version	–
Source(s)	Avis de sécurité Cisco 105444 du 04 juin 2008
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

- Dénis de service à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- Cisco ASA et PIX pour les versions de la branche 7.1.x antérieures à 7.1(2)70 ;
- Cisco ASA et PIX pour les versions de la branche 7.2.x antérieures à 7.2(4) ;
- Cisco ASA et PIX pour les versions de la branche 8.0.x antérieures à 8.0(3)10 ;
- Cisco ASA et PIX pour les versions de la branche 8.1.x antérieures à 8.1(1)2.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans les équipements réseaux de sécurité Cisco PIX (*Private Internet EXchange*) et Cisco ASA (*Adaptive Security Appliance*). Celles-ci peuvent être exploitées à distance par le biais de trames spécialement construites afin de perturber le fonctionnement de l'équipement. Une autre vulnérabilité offre la possibilité de contourner la politique de sécurité mise en place au moyen de listes d'accès.

4 Description

Plusieurs vulnérabilités ont été identifiées dans les équipements réseaux de sécurité Cisco PIX (*Private Internet EXchange*) et Cisco ASA (*Adaptive Security Appliance*) :

- les trames d'accusé de réception TCP ACK ne sont pas correctement interprétées lorsqu'elles sont adressés à l'interface de l'équipement. L'exploitation de cette vulnérabilité peut perturber le fonctionnement du système ;
- les requêtes TLS (*Transport Layer Security*) ne sont pas correctement interprétées lorsqu'elles sont adressées au serveur Web (HTTPS) de l'équipement. L'exploitation de cette vulnérabilité peut perturber le fonctionnement du système ;
- certaines trames de messagerie instantanée ne sont pas correctement interprétées par le moteur d'inspection de l'équipement. L'exploitation de cette vulnérabilité peut perturber le fonctionnement du système ;
- le système ne gère pas correctement des tentatives de balayage adressées à l'équipement sur le port 443/tcp ;
- des règles de contrôles d'accès pourraient être contournées sous certaines conditions non spécifiées par l'éditeur.

5 Solution

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

6 Documentation

- Bulletin de sécurité Cisco 20080604-asa (105444) du 04 juin 2008 :
<http://www.cisco.com/warp/public/707/cisco-sa-20080604-asa.shtml>
- Référence CVE CVE-2008-2055 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2055>
- Référence CVE CVE-2008-2056 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2056>
- Référence CVE CVE-2008-2057 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2057>
- Référence CVE CVE-2008-2058 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2058>
- Référence CVE CVE-2008-2059 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2059>

Gestion détaillée du document

05 juin 2008 version initiale.