

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités des équipements Cisco ASA et PIX.

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-441>

Gestion du document

Référence	CERTA-2008-AVI-441
Titre	Multiples vulnérabilités des équipements Cisco ASA et PIX.
Date de la première version	04 septembre 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco #107475 du 03 septembre 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 ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- Cisco Adaptive Security Appliance (ASA) 7.x ;
- Cisco Adaptive Security Appliance (ASA) 8.x ;
- Cisco PIX 7.x ;
- Cisco PIX 8.x.

3 Résumé

Plusieurs vulnérabilités présentes dans les produits ASA et PIX de Cisco permettent à un utilisateur distant de provoquer un déni de service ou de porter atteinte à la confidentialité de certaines données.

4 Description

De multiples vulnérabilités sont présentes dans les produits ASA et PIX de Cisco :

- la première est relative à la mise en œuvre du protocole SIP et permet à un utilisateur distant de provoquer un redémarrage intempestif du système vulnérable ;
- la seconde est relative à la gestion des connexions de clients VPN et permet également de provoquer un déni de service de l'équipement ;
- la troisième est due à une fuite mémoire dans le composant gérant les paquets SSL ou HTTP et permet de provoquer un arrêt inopiné du système ;
- la quatrième est relative à une erreur dans la manipulation de certaines URI particulières utilisées dans le cadre d'accès VPN et peut causer également un déni de service ;
- la dernière permet à un utilisateur distant de collecter certaines données du système en incitant un utilisateur à visiter un site web construit de façon particulière ou à répondre à un courriel particulier.

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 ID 10475 du 03 septembre 2008 :
<http://www.cisco.com/warp/public/707/cisco-sa-20080903-asa.shtml>
- Référence CVE CVE-2008-2732 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2732>
- Référence CVE CVE-2008-2733 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2733>
- Référence CVE CVE-2008-2734 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2734>
- Référence CVE CVE-2008-2735 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2735>
- Référence CVE CVE-2008-2736 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2736>

Gestion détaillée du document

04 septembre 2008 version initiale.