



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 février 2007
N° CERTA-2007-AVI-090-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de produits Cisco

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-2007-AVI-090>

Gestion du document

Référence	CERTA-2007-AVI-090-001
Titre	Multiples vulnérabilités de produits Cisco
Date de la première version	16 février 2007
Date de la dernière version	27 février 2007
Source(s)	Bulletins Cisco du 14 février 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 PIX 500 versions 6.x et 7.x ;
- Cisco ASA 5500 versions 7.x ;
- Cisco Firewall Service Module (FWSM) versions 2.x et 3.x.

3 Résumé

Plusieurs vulnérabilités sur les produits *Cisco PIX*, *ASA* et *FWSM* permettent de réaliser un déni de service à distance, de contourner la politique de sécurité ou d'élever ses privilèges.

4 Description

Plusieurs vulnérabilités affectent les produits *Cisco* précités :

- une erreur dans la méthode d’authentification LOCAL de *PIX 6.x* permet à un utilisateur authentifié malveillant disposant des privilèges minimaux (`level 0`) d’obtenir les privilèges maximaux (`level 15`);
- une erreur dans la gestion des listes de contrôle d’accès (*ACL*) par *FWSM* permet à un utilisateur malveillant de ne pas faire évaluer des règles de contrôle d’accès ou de les faire évaluer dans un ordre incorrect;
- une erreur dans le traitement des paquets SIP malformés provoque un rechargement du système ou un arrêt inopiné. Un utilisateur malveillant peut provoquer un déni de service à distance au moyen d’un paquet SIP conçu à cet effet;
- une erreur dans l’inspection du trafic HTTP, quand cette inspection est activée, provoque le rechargement ou l’arrêt du système. Un utilisateur malveillant peut provoquer un déni de service à distance au moyen d’une communication HTTP conçue à cet effet;
- une erreur dans l’inspection du trafic des protocoles basés sur TCP, quand cette inspection est activée, provoque le rechargement ou l’arrêt du système. Un utilisateur malveillant peut provoquer un déni de service à distance au moyen d’une communication basée sur TCP (HTTP, FTP...) conçue à cet effet;
- Plusieurs erreurs affectant le traitement des requêtes HTTPS, SNMP et HTTP (URL longues) par *FWSM 3.x* provoquent le rechargement du système. Dans certaines conditions, un utilisateur malveillant peut provoquer un déni de service à distance au moyen de trafic conçu à cet effet.

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 72327 du 14 février 2007 :
http://www.cisco.com/en/US/products/products_security_advisory09186a00807e2481.shtml
- Bulletin de sécurité Cisco ID 77853 du 14 février 2007 :
http://www.cisco.com/en/US/products/products_security_advisory09186a00807e2484.shtml
- Référence CVE CVE-2007-0959
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0959>
- Référence CVE CVE-2007-0960
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0960>
- Référence CVE CVE-2007-0961
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0961>
- Référence CVE CVE-2007-0962
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0962>
- Référence CVE CVE-2007-0963
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0963>
- Référence CVE CVE-2007-0964
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0964>
- Référence CVE CVE-2007-0965
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0965>
- Référence CVE CVE-2007-0966
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0966>
- Référence CVE CVE-2007-0967
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0967>
- Référence CVE CVE-2007-0968
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0968>

Gestion détaillée du document

16 février 2007 version initiale.

27 février 2007 correction des liens.