



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 juillet 2006
N° CERTA-2006-AVI-290

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Cisco IPS

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-2006-AVI-290>

Gestion du document

Référence	CERTA-2006-AVI-290
Titre	Vulnérabilité de Cisco IPS
Date de la première version	13 juillet 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco du 12 juillet 2006
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.

2 Systèmes affectés

- Logiciel Cisco IPS version 5.1(1) ;
- logiciel Cisco IPS version 5.1(1a) ;
- logiciel Cisco IPS version 5.1(1b) ;
- logiciel Cisco IPS version 5.1(1c) ;
- logiciel Cisco IPS version 5.1(1d) ;
- logiciel Cisco IPS version 5.1(1e) ;
- logiciel Cisco IPS version 5.1(p1).

Le logiciel Cisco IPS (pour *Intrusion Prevention System*) est installé dans plusieurs produits Cisco, tels :

- IDS-4235 ;
- IPS-4240 ;
- IDS-4250 (SX/TX/XL) ;
- IPS-4255.

3 Description

Cisco IPS (*Intrusion Prevention System*) est un matériel de sécurité notamment destiné au filtrage. Une vulnérabilité a été identifiée dans un pilote de l'adaptateur chargé d'analyser les paquets capturés par les interfaces : il ne traiterai pas correctement certains paquets IP malformés. Une personne malveillante peut envoyer l'un d'entre eux sur un système vulnérable, ce qui provoquerait alors l'arrêt du traitement des paquets et nécessiterait le redémarrage du matériel.

4 Solution

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

5 Documentation

- Bulletin de sécurité Cisco ID 70653 du 12 juillet 2006 :
<http://www.cisco.com/warp/public/707/cisco-sa-20060712-ips.shtml>

Gestion détaillée du document

13 juillet 2006 version initiale.