

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de certaines couches protocolaires dans Cisco IOS

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-050>

Gestion du document

Référence	CERTA-2007-AVI-050-001
Titre	Vulnérabilités de certaines couches protocolaires dans Cisco IOS
Date de la première version	24 janvier 2007
Date de la dernière version	25 janvier 2007
Source(s)	Bulletins de sécurité Cisco du 24 janvier 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 ;
- Exécution de code arbitraire à distance.

2 Systèmes affectés

- Toutes les versions de CISCO IOS Software (9.x, 10.x, 11.x et 12.x).

3 Description

Plusieurs vulnérabilités ont été identifiées dans le système d'exploitation Cisco IOS. Elles touchent les couches protocolaires TCP, IPv4 et IPv6 :

- la couche TCP ne manipulerait pas correctement les numéros de séquence et les valeurs acquittées ; une personne malveillante pourrait envoyer plusieurs paquets exploitant cette vulnérabilité, afin de provoquer un déni de service ;
- la couche IPv4 ne manipulerait pas correctement le champ `IP option`. Une personne malveillante pourrait ainsi envoyer un paquet avec une en-tête IP contenant un champ mal conçu et une autre en-tête particulière ICMP, PIMv2, PGM ou URD afin d'exécuter du code arbitraire à distance ;

- la couche IPv6 ne manipulerait pas correctement des options de routage par la source (Type 0 Routing Headers), pouvant conduire à un dysfonctionnement du système vulnérable.

4 Solution

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

5 Documentation

- Bulletin de sécurité Cisco ID 72318 du 24 janvier 2007 :
<http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-tcp.shtml>
- Bulletin de sécurité Cisco ID 81734 du 24 janvier 2007 :
<http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml>
- Bulletin de sécurité Cisco ID 72372 du 24 janvier 2007 :
<http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOI-IPv6.shtml>
- Référence CVE CVE-2007-0479 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0479>
- Référence CVE CVE-2007-0480 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0480>
- Référence CVE CVE-2007-0481 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0481>

Gestion détaillée du document

24 janvier 2007 version initiale.

25 janvier 2007 ajout des références CVE et modification des risques.