

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Cisco IPSEC VPN Services Module

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-2004-AVI-125>

Gestion du document

Référence	CERTA-2004-AVI-125
Titre	Vulnérabilité de Cisco IPSEC VPN Services Module
Date de la première version	09 avril 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité de Cisco : "Cisco IPSEC VPN Services Module malformed IKE packet vulnerability"
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.

2 Systèmes affectés

Commutateurs Cisco Catalyst 6500 et routeurs Cisco 7600 avec les versions d'IOS suivantes :

- versions antérieures à 12.2(17b)SXA ;
- versions antérieures à 12.2(17d)SXB ;
- versions antérieures à 12.2(14)SY03.

3 Résumé

A l'aide de paquets IKE habilement constitués, un utilisateur mal intentionné peut réaliser un déni de service sur les Commutateurs Cisco Catalyst 6500 et routeurs Cisco 7600 utilisant le module VPNSM (IPSec Services Module).

4 Description

Le module VPNISM (IPSec Services Module) est une carte intégrable dans les Commutateurs Cisco Catalyst 6500 et routeurs Cisco 7600. VPNISM offre le support des fonctionnalités IPSec.

Selon Cisco, à l'aide de paquets IKE habilement constitués, un utilisateur mal intentionné peut réaliser un déni de service provoquant le redémarrage à chaud de ces équipements.

5 Solution

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

6 Documentation

Bulletin de sécurité "Cisco IPSEC VPN Services Module malformed IKE packet vulnerability" de Cisco :
<http://www.cisco.com/warp/public/707/cisco-sa-20040408-vpnsn.shtml>

Gestion détaillée du document

09 avril 2004 version initiale.