

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités des 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-2009-AVI-377>

Gestion du document

Référence	CERTA-2009-AVI-377
Titre	Vulnérabilités des produits Cisco
Date de la première version	09 septembre 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco 20090908-tcp24 du 08 septembre 2009
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

- Cisco IOS ;
- Cisco IOS-XE ;
- Cisco CatOS ;
- Cisco ASA ;
- Cisco PIX ;
- Cisco NX-OS ;
- gamme Scientific Atlanta ;
- gamme Lynksys.

3 Résumé

Plusieurs produits Cisco présentent des vulnérabilités permettant à un utilisateur malveillant de provoquer un déni de service à distance.

4 Description

Plusieurs vulnérabilités des produits *Cisco* ont été publiées :

- (CVE-2008-4609) les produits listés en section « systèmes affectés » présentent des faiblesses dans le traitement du protocole TCP. Celles-ci permettent à un attaquant de provoquer un déni de service à distance par épuisement des ressources utilisées dans la gestion du protocole TCP ;
- (CVE-2009-0627) les systèmes *Cisco NX-OS* sur plateforme *Cisco Nexus 5000* peuvent s'arrêter de manière inopinée lors de la réception d'une séquence particulière TCP. Ce défaut est exploitable par un attaquant pour provoquer un déni de service à distance.

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 20090908-tcp24 du 08 septembre 2009 :
<http://www.cisco.com/warp/public/707/cisco-sa-20090908-tcp24.shtml>
- Référence CVE CVE-2008-4609 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4609>
- Référence CVE CVE-2009-0627 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0627>

Gestion détaillée du document

09 septembre 2009 version initiale.