

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans les commutateurs Cisco Nexus 5000 et 3000 series

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-2011-AVI-499>

Gestion du document

Référence	CERTA-2011-AVI-499
Titre	Vulnérabilité dans les commutateurs Cisco Nexus 5000 et 3000 series
Date de la première version	08 septembre 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco 20110907-nexus du 07 septembre 2011
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

Contournement de la politique de sécurité.

2 Systèmes affectés

- Cisco Nexus 5000 NX-OS Software versions 5.0(2) et 5.0(3) antérieures à la version 5.0(3)N2(1) ;
- Cisco Nexus 3000 NX-OS Software versions antérieures à la 5.0(3)U1(2a) ou 5.0(3)U2(1).

3 Résumé

Une vulnérabilité dans les commutateurs Cisco Nexus 5000 et 3000 series permet à une personne malintentionnée de contourner la politique de sécurité.

4 Description

Une vulnérabilité dans les commutateurs Cisco Nexus 5000 et 3000 series permet de contourner le rejet du trafic configuré dans les *ACL (Access Control Lists)*.

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 20110907-nexus du 07 septembre 2011 :
<http://www.cisco.com/warp/public/707/cisco-sa-20110907-nexus.shtml>
- Référence CVE CVE-2011-2581 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2581>

Gestion détaillée du document

08 septembre 2011 version initiale.