



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 21 septembre 2011  
N° CERTA-2011-AVI-488-001

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans les 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-2011-AVI-488>

---

### Gestion du document

Référence	CERTA-2011-AVI-488-001
Titre	Vulnérabilité dans les produits Cisco
Date de la première version	01 septembre 2011
Date de la dernière version	21 septembre 2011
Source(s)	Bulletin de sécurité Cisco cisco-sa-20110830-apache
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 MDS 9000 NX-OS versions antérieures à la 4.2 ;
- Cisco NX-OS Software pour Cisco Nexus 7000 Series Switches versions antérieures à la 5.1 ;
- Cisco SAN-OS 3.x ;
- Cisco TelePresence Video Communication Server (Cisco TelePresence VCS) ;
- Tous les systèmes Cisco CTS TelePresence ;
- Cisco Video Surveillance Manager (VSM) ;
- Cisco Video Surveillance Operations Manager (VSOM) ;
- Management Center for Cisco Security Agent ;
- Cisco Wireless Control System (WCS) ;
- Cisco Wild Area Application Services (WAAS) Software ;
- Cisco Quad ;
- Cisco Network Collector ;
- Cisco Mobility Services Engine ;

- CiscoWorks Common Services ;
- CiscoWorks LAN Management Solution.

### 3 Résumé

Une vulnérabilité dans Cisco NX-OS peut être utilisée pour réaliser un déni de service à distance.

### 4 Description

Une vulnérabilité a été corrigée dans Cisco NX-OS. Cette vulnérabilité affecte le serveur `httpd` Apache. Elle peut être utilisée à l'aide de requêtes *HTTP* spécialement conçues (utilisation de l'entête *range* avec des intervalles se chevauchant) 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 20110830-apache du 30 août 2011 :  
<http://www.cisco.com/warp/public/707/cisco-sa-20110830-apache.shtml>
- Référence CVE CVE-2011-3192 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192>

## Gestion détaillée du document

**01 septembre 2011** version initiale.

**21 septembre 2011** modification du titre et ajout de systèmes vulnérables.