

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité du serveur TFTP des équipements 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-197>

---

### Gestion du document

Référence	CERTA-2009-AVI-197
Titre	Vulnérabilité du serveur TFTP des équipements Cisco
Date de la première version	26 mai 2009
Date de la dernière version	–
Source(s)	Bulletins de sécurité Cisco #110143 et #110288
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 ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

- Cisco Security Manager (CSM) 3.x ;
- Cisco TelePresence Readiness Assessment Manager (CTRAM) 1.x ;
- Cisco Unified Operations Manager (CUOM) 1.x ;
- Cisco Unified Operations Manager (CUOM) 2.x ;
- Cisco Unified Provisioning Manager 1.x ;
- Cisco Unified Service Monitor (CUSM) 1.x ;
- Cisco Unified Service Monitor (CUSM) 2.x ;
- CiscoWorks Common Services Software 3.x ;
- CiscoWorks Health and Utilization Monitor 1.x ;
- CiscoWorks LAN Management Solution (LMS) 2.x ;
- CiscoWorks LAN Management Solution (LMS) 3.x ;

- CiscoWorks QoS Policy Manager (QPM) 4.x ;
- CiscoWorks Voice Manager 3.x.

### **3 Résumé**

Une vulnérabilité présente dans le serveur TFTP de certains équipements Cisco permet à un utilisateur distant malintentionné de contourner la politique de sécurité et de porter atteinte à la confidentialité ou à l'intégrité des données.

### **4 Description**

Un manque de contrôle dans les entrées passées au serveur TFTP de certains produits Cisco permet à un utilisateur distant de déposer ou de récupérer des fichiers en dehors de la racine de ce serveur. Ce faisant, il peut accéder à la configuration de l'équipement ou modifier cette dernière.

### **5 Solution**

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

### **6 Documentation**

- Bulletins de sécurité Cisco #110143 et #110288 du 20 mai 2009 :  
<http://www.cisco.com/warp/public/707/cisco-sa-20090520-cw.shtml>  
<http://www.cisco.com/warp/public/707/cisco-amb-20090520-cw.shtml>

### **Gestion détaillée du document**

**26 mai 2009** version initiale.