



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 octobre 2011  
N° CERTA-2011-AVI-583

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans CiscoWorks Common Services

---

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-583>

---

### Gestion du document

Référence	CERTA-2011-AVI-583
Titre	Vulnérabilité dans CiscoWorks Common Services
Date de la première version	21 octobre 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20111019-cs du 19 octobre 2011T
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

Élévation de privilèges.

## 2 Systèmes affectés

- CiscoWorks LAN Management Solutions 3.x et 4.x pour Windows intégrant Common Services versions inférieures à la version 4.1 ;
- Cisco Security Manager 3.x et 4.x intégrant Common Services versions inférieures à la version 4.1 ;
- Cisco Unified Operations Manager 2.x et 8.x intégrant Common Services versions inférieures à la version 4.1 ;
- Cisco Unified Service Monitor 2.x et 8.x intégrant Common Services versions inférieures à la version 4.1 ;
- CiscoWorks Quality of Service Policy Manager 4.x pour Windows intégrant Common Services versions inférieures à la version 4.1 ;
- CiscoWorks Voice Manager 3.x pour Windows intégrant Common Services versions inférieures à la version 4.1.

### **3 Résumé**

Une vulnérabilité a été corrigée dans Cisco Common Services et permet à une personne malintentionnée d'exécuter des commandes avec les privilèges de l'administrateur système.

### **4 Description**

Une vulnérabilité a été corrigée dans Cisco Common Services. Elle permet à un personne malintentionnée et authentifiée sur le système d'exécuter des commandes avec les privilèges de l'administrateur système au moyen d'une URL spécialement conçue.

### **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 20111019-cs du 19 octobre 2011 :  
<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20111019-cs>
- Référence CVE CVE-2011-3310 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3310>

### **Gestion détaillée du document**

**21 octobre 2011** version initiale.