



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 27 janvier 2011  
N° CERTA-2011-AVI-033

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans Cisco Content Service Gateway

---

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-033>

---

### Gestion du document

Référence	CERTA-2011-AVI-033
Titre	Multiples vulnérabilités dans Cisco Content Service Gateway
Date de la première version	27 janvier 2011
Date de la dernière version	–
Source(s)	Avis Cisco-sa-20110126-csg2
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 ;
- contournement de la politique de sécurité.

## 2 Systèmes affectés

Cisco Content Service Gateway deuxième génération (CSG2).

## 3 Résumé

Plusieurs vulnérabilités sont présentes dans Cisco Content Service Gateway CSG2. Elles permettent de contourner la politique de sécurité (accès à des sites non autorisés, non facturation de l'accès), ou de provoquer un déni de service à distance.

## 4 Description

Plusieurs vulnérabilités sont présentes dans Cisco Content Service Gateway.

- L'envoi d'un paquet TCP particulier peut entraîner un déni de service sur la passerelle ;

- L'envoi d'une requête HTTP particulière, après avoir accédé à un site autorisé, permet un contournement de la politique de sécurité en place. Il est ainsi possible d'accéder à des sites normalement interdits ou de contourner le système de facturation. Cette vulnérabilité ne concerne que le trafic HTTP et non les autres protocoles tel que HTTPS.

## **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 20110126-csg2 du 26 janvier 2011 :  
<http://www.cisco.com/warp/public/707/cisco-sa-20110126-csg2.shtml>
- Référence CVE CVE-2011-0348 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0348>
- Référence CVE CVE-2011-0349 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0349>
- Référence CVE CVE-2011-0350 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0350>

## **Gestion détaillée du document**

**27 janvier 2011** version initiale.