Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 07 juillet 2011
N° CERTA-2011-AVI-382

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Cisco Content Services Gateway

Gestion du document

Référence	CERTA-2011-AVI-382
Titre	Vulnérabilité dans Cisco Content Services Gateway
Date de la première version	07 juillet 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité cisco-sa-20110706-csg du 06 juillet 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

Déni de service à distance.

2 Systèmes affectés

Cisco Content Services Gateway: Second Generation.

3 Résumé

Une vulnérabilité dans *Cisco Content Services Gateway* permet de réaliser un déni de service à distance.

4 Description

Une vulnérabilité a été découverte dans *Cisco Content Services Gateway*. Un attaquant peut, sans authentification préalable, provoquer le redémarrage du dispositif en envoyant une série de paquets ICMP.

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 20110706-csg du 06 juillet 2011 :
  http://www.cisco.com/warp/public/707/cisco-sa-20110706-csg.shtml
- Référence CVE CVE-2011-2064 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2064

Gestion détaillée du document

07 juillet 2011 version initiale.