



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 25 août 2011
N° CERTA-2011-AVI-469

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Cisco IOS

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-469>

Gestion du document

Référence	CERTA-2011-AVI-469
Titre	Vulnérabilité dans Cisco IOS
Date de la première version	25 août 2011
Date de la dernière version	–
Source(s)	Notes de mise à jour Cisco du 04 août 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 IOS 12.x.

3 Résumé

Une vulnérabilité permettant à une personne malintentionnée d'effectuer un déni de service à distance a été découverte dans *Cisco IOS*.

4 Description

Une vulnérabilité a été découverte dans *Cisco IOS*. Elle permet à une personne malintentionnée d'effectuer un déni de service à distance lors de l'établissement de deux connexions ssh2. Bien que la cause exacte de cette faille ne soit pas connue, l'éditeur précise qu'elle est liée à l'utilisation de bannières personnalisées.

5 Solution

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

6 Documentation

- Notes de mise à jour *Cisco* du 04 août 2011 :
http://www.cisco.com/en/US/docs/switches/lan/cisco_ie3000/software/release/12.2_58_se/release/notes/OL24335.html
- Référence CVE CVE-2011-1624 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1624>

Gestion détaillée du document

25 août 2011 version initiale.