

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans des caméras 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-2011-AVI-602>

Gestion du document

Référence	CERTA-2011-AVI-602
Titre	Vulnérabilité dans des caméras Cisco
Date de la première version	28 octobre 2011
Date de la dernière version	–
Source	Bulletin de sécurité Cisco 20111026-camera du 26 octobre 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

Caméra de vidéosurveillance Cisco, séries 2421, 2500 et 2600.

3 Résumé

Une vulnérabilité dans des caméras de vidéosurveillance Cisco permet à un utilisateur malveillant de réaliser un déni de service à distance.

4 Description

Les caméras de vidéosurveillance Cisco des séries vulnérables ne traitent pas correctement des paquets RTSP mal formés. Cette vulnérabilité est exploitable par un utilisateur malintentionné pour provoquer à distance un arrêt avec redémarrage de l'appareil vulnérable.

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 20111026-camera du 26 octobre 2011 :
<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20111026-camera>
- Référence CVE CVE-2011-3318 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3318>

Gestion détaillée du document

28 octobre 2011 version initiale.