

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de produits Cisco Video Surveillance

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-2009-AVI-255>

Gestion du document

Référence	CERTA-2009-AVI-255
Titre	Vulnérabilités de produits Cisco Video Surveillance
Date de la première version	25 juin 2009
Date de la dernière version	–
Source(s)	
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 ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- Cisco Video Surveillance Stream Manager for the Cisco Video Surveillance Services Platform, versions antérieures à la version 5.3 ;
- Cisco Video Surveillance Stream Manager for the Cisco Video Surveillance Integrated Services Platform, versions antérieures à la version 5.3 ;
- Cisco Video Surveillance 2500 Series IP Camera firmware, versions antérieures à la version 2.1.

3 Résumé

Des vulnérabilités affectent des produits de vidéosurveillance Cisco et permettent à un utilisateur malveillant de provoquer un déni de service à distance ou de lire indûment des informations.

4 Description

Une vulnérabilité est présente dans Cisco Video Surveillance Stream Manager (CVE-2009-2045). Un utilisateur malveillant peut provoquer un redémarrage du système par le biais d'un paquet UDP particulier sur le port 37000.

Une vulnérabilité affecte les caméras IP de la série 2500, avec ou sans fil (CVE-2009-2046). Un utilisateur authentifié peut lire tout fichier présent sur la caméra au travers du serveur web embarqué, via le port 80 (HTTP) ou le port 443 (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 20090624-video du 24 juin 2009 :
<http://www.cisco.com/warp/public/707/cisco-sa-20090624-video.shtml>
- Référence CVE CVE-2009-2045 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2045>
- Référence CVE CVE-2009-2046 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2046>

Gestion détaillée du document

25 juin 2009 version initiale.