

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Cisco TelePresence Video Communication Server

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-2012-AVI-109>

Gestion du document

Référence	CERTA-2012-AVI-109
Titre	Vulnérabilités dans Cisco TelePresence Video Communication Server
Date de la première version	01 mars 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco 20120229-vcs du 29 février 2012
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 TelePresence Video Communication Server (Control, Expressway et Starter Pack Express).

3 Résumé

Des vulnérabilités dans *Cisco TelePresence Video Communication Server* permettent de réaliser un déni de service à distance.

4 Description

Des vulnérabilités ont été découvertes dans la gestion des paquets SIP (*Session Initiation Protocol*) dans *Cisco TelePresence Video Communication Server*. L'exploitation de ces vulnérabilités, par le biais de paquets SIP envoyés au port 5060 et 5061 (TCP et UDP), permet de réaliser un déni de service à distance.

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 20120229-vcv du 29 février 2012 :
<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120229-vcv>
- Référence CVE CVE-2012-0330 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0330>
- Référence CVE CVE-2012-0331 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0331>

Gestion détaillée du document

01 mars 2012 version initiale.