

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Cisco ASA 1000V Cloud Firewall H.323

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-2013-AVI-044>

Gestion du document

Référence	CERTA-2013-AVI-044
Titre	Vulnérabilité dans Cisco ASA 1000V Cloud Firewall H.323
Date de la première version	17 janvier 2013
Date de la dernière version	–
Source(s)	Bulletin de sécurité CISCO CSCuc42812 du 16 janvier 2013
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 ASA 1000V Cloud Firewall Software 8.7 Base
- Cisco ASA 1000V Cloud Firewall Software 8.7.1.1

3 Résumé

Une vulnérabilité a été corrigée dans *Cisco ASA 1000V Cloud Firewall H.323*. Elle permet à un attaquant de provoquer un déni de service à distance au moyen de messages H.323 spécialement conçus.

4 Solution

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

5 Documentation

- Bulletin de sécurité CISCO CSCuc42812 du 16 janvier 2013 :
<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130116-asa1000v>
- Référence CVE CVE-2012-5419
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5419>

Gestion détaillée du document

17 janvier 2013 version initiale.