

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans CISCO ASA 5500

---

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-144>

---

### Gestion du document

Référence	CERTA-2012-AVI-144
Titre	Vulnérabilité dans CISCO ASA 5500
Date de la première version	15 mars 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco 20120314-asaclient du 15 mars 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

Exécution de code arbitraire à distance.

## 2 Systèmes affectés

- CISCO ASA 5500 Series Adaptive Security Appliance Software 7.1 et 7.2 ;
- CISCO ASA 5500 Series Adaptive Security Appliance Software 8.6 et antérieures.

## 3 Résumé

Une vulnérabilité a été corrigée dans CISCO ASA 5500 Series Adaptive Security Appliance, qui peut être exploitée pour exécuter du code arbitraire à distance.

## 4 Description

Une vulnérabilité a été corrigée dans les contrôles ActiveX de la fonctionnalité « Clientless VPN » utilisée dans CISCO ASA 5500 Series Adaptive Security Appliance. Tout utilisateur ayant sollicité une fois cette fonctionnalité a téléchargé un ActiveX vulnérable. Un attaquant distant peut alors, en incitant l'utilisateur à naviguer sur un site spécialement conçu, exécuter du code arbitraire sur la machine de l'utilisateur.

## **5 Solution**

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation). Les utilisateurs de cette fonctionnalité avant la mise en place du correctif restent vulnérables et devront utiliser les solutions de contournement indiquées dans ce bulletin de sécurité.

## **6 Documentation**

- Bulletin de sécurité Cisco 20120314-asacient du 15 mars 2012 :  
<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120314-asacient>
- Référence CVE CVE-2012-0358 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0358>

## **Gestion détaillée du document**

**15 mars 2012** version initiale.