

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans les produits Cisco SA 500 Series Security Appliances

---

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-404>

---

### Gestion du document

Référence	CERTA-2011-AVI-404
Titre	Vulnérabilités dans les produits Cisco SA 500 Series Security Appliances
Date de la première version	21 juillet 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco 20110720-sa500 du 20 juillet 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

- Atteinte à la confidentialité des données ;
- élévation de privilèges.

## 2 Systèmes affectés

- Cisco SA520 ;
- Cisco SA520W ;
- Cisco SA540.

## 3 Résumé

Deux vulnérabilités dans les produits Cisco SA 500 Series Security Appliances permettent à une personne malintentionnée soit d'élever ses privilèges, soit de porter atteinte à la confidentialité des données.

## 4 Description

Deux vulnérabilités dans les produits Cisco SA 500 Series Security Appliances ont été découvertes :

- la première permet à une personne distante non authentifiée de porter atteinte à la confidentialité des données d'identification via une injection de code *SQL* (CVE-2011-2546) ;
- la seconde permet à un utilisateur authentifié d'élever ses privilèges sur le système par l'envoi de paramètres spécifiques via des formulaires web (CVE-2011-2547).

## 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 20110720-sa500 du 20 juillet 2011 :  
<http://www.cisco.com/warp/public/707/cisco-sa-20110720-sa500.shtml>
- Référence CVE CVE-2011-2546 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2546>
- Référence CVE CVE-2011-2547 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2547>

## Gestion détaillée du document

21 juillet 2011 version initiale.