



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

**S . G . D . S . N**  
Agence nationale de la sécurité  
des systèmes d'information  
CERTA

Paris, le 13 mars 2008  
N° CERTA-2008-AVI-133

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans Cisco User-Changeable Password

---

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-2008-AVI-133>

---

### Gestion du document

Référence	CERTA-2008-AVI-133
Titre	Multiples vulnérabilités dans Cisco User-Changeable Password
Date de la première version	13 mars 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco 20080312-ucp du 12 mars 2008
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 ;
- exécution de code arbitraire à distance ;
- injection de code indirecte (XSS).

## 2 Systèmes affectés

Cisco User-Changeable Password 4.x.

## 3 Résumé

Plusieurs vulnérabilités dans Cisco User-Changeable Password permettent d'effectuer un déni de service à distance et une injection de code indirecte.

## 4 Description

Plusieurs vulnérabilités ont été identifiées dans Cisco User-Changeable Password. Plusieurs vulnérabilités dans le script UCP CGI permettent à un individu malveillant d'effectuer un dépassement de mémoire tampon, une exécution de code arbitraire à distance ou une injection de code indirecte.

## 5 Solution

Se référer au bulletin de sécurité Cisco 20080312-ucp pour l'obtention des correctifs (cf. section Documentation).

## 6 Documentation

- Bulletin de sécurité Cisco 20080312-ucp du 12 mars 2008 :  
<http://www.cisco.com/warp/public/707/cisco-sa-20080312-ucp.shtml>
- Référence CVE CVE-2008-0532 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0532>
- Référence CVE CVE-2008-0533 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0533>

## Gestion détaillée du document

**13 mars 2008** version initiale.