



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 21 juin 2010  
N° CERTA-2010-AVI-275

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans CUPS

---

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-2010-AVI-275>

---

### Gestion du document

Référence	CERTA-2010-AVI-275
Titre	Vulnérabilités dans CUPS
Date de la première version	21 juin 2010
Date de la dernière version	–
Source(s)	
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 ;
- contournement de la politique de sécurité ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

CUPS 1.x.

## 3 Résumé

Plusieurs vulnérabilités dans CUPS permettent à un utilisateur malintentionné de contourner la politique de sécurité, de porter atteinte à la confidentialité des données ou d'exécuter du code arbitraire à distance.

## 4 Description

Trois vulnérabilités dans CUPS ont été corrigées.

- Une vulnérabilité causée par un manque de contrôle lors d'une allocation de mémoire peut être exploitée afin d'exécuter du code arbitraire ;
- une vulnérabilité peut être exploitée au travers de l'interface Web CUPS afin de porter atteinte à la confidentialité des données (CVE-2010-1748) ;
- une vulnérabilité permet à un utilisateur malveillant de contourner la politique de sécurité afin de modifier certains paramètres de configuration (CVE-2010-0540).

## **5 Solution**

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

## **6 Documentation**

- Annonce de mise à jour CUPS du 17 juin 2010 :  
<http://cups.org/articles.php?L596>
- Référence CVE CVE-2010-0540 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0540>
- Référence CVE CVE-2010-0542 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0542>
- Référence CVE CVE-2010-1748 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1748>

## **Gestion détaillée du document**

**21 juin 2010** version initiale.