



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 11 mai 2009  
N° CERTA-2009-AVI-156-001

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples 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-2009-AVI-156>

---

### Gestion du document

Référence	CERTA-2009-AVI-156-001
Titre	Multiples vulnérabilités dans cups
Date de la première version	21 avril 2009
Date de la dernière version	11 mai 2009
Source(s)	Note de changements CUPS du 16 avril 2009
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 ;
- déni de service à distance ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

- CUPS 1.x.

## 3 Résumé

Plusieurs vulnérabilités découvertes dans CUPS permettent à un utilisateur distant malveillant d'exécuter du code arbitraire ou de porter atteinte à la confidentialité des données.

## 4 Description

Plusieurs vulnérabilités présentes dans la commande `pdf tops`, causées par l'usage de code source vulnérable issu de `Xpdf`, peuvent être exploitées afin de provoquer un déni de service ou d'exécuter du code arbitraire à distance.

Une vulnérabilité de type débordement d'entier durant le traitement d'un fichier au format `TIFF` peut être exploitée au moyen d'un fichier spécialement construit afin d'exécuter du code arbitraire à distance.

Une erreur dans le traitement des en-têtes `Host` : permet à une personne malveillante de porter atteinte à la confidentialité des données telles que l'historique des travaux d'impression.

## 5 Solution

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

## 6 Documentation

- Note de changements CUPS du 16 avril 2009 :  
<http://cups.org/articles.php?L582>
- Notes de sécurité CUPS STR #3031 et #3118 du 16 avril 2009 :  
<http://cups.org/str.php?L3031>  
<http://cups.org/str.php?L3118>
- Bulletin de sécurité Gentoo GLSA-200904-20 du 23 avril 2009 :  
<http://www.gentoo.org/security/en/glsa/glsa-200904-20.xml>
- Bulletin de sécurité Debian DSA-1773 du 17 avril 2009 :  
<http://www.debian.org/security/2009/dsa-1773>
- Bulletin de sécurité Debian DSA-1790 du 05 mai 2009 :  
<http://www.debian.org/security/2009/dsa-1790>
- Bulletin de sécurité Debian DSA-1793 du 06 mai 2009 :  
<http://www.debian.org/security/2009/dsa-1793>
- Bulletin de sécurité RedHat RHSA-2009:0429-1 du 16 avril 2009 :  
<http://rhn.redhat.com/errata/RHSA-2009-0429.html>
- Bulletin de sécurité RedHat RHSA-2009:0430-1 du 16 avril 2009 :  
<http://rhn.redhat.com/errata/RHSA-2009-0430.html>
- Bulletin de sécurité RedHat RHSA-2009:0431-1 du 16 avril 2009 :  
<http://rhn.redhat.com/errata/RHSA-2009-0431.html>
- Bulletin de sécurité RedHat RHSA-2009:0458-1 du 30 avril 2009 :  
<http://rhn.redhat.com/errata/RHSA-2009-0458.html>
- Bulletin de sécurité Ubuntu USN-759-1 et USN-760-1 du 16 avril 2009 :  
<http://www.ubuntu.com/usn/usn-759-1>  
<http://www.ubuntu.com/usn/usn-760-1>
- Bulletin de sécurité SuSE SUSE-SA:2009:024 du 22 avril 2009 :  
<http://lists.opensuse.org/opensuse-security-announce/2009-04/msg00011.html>
- Référence CVE CVE-2009-0146 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0146>
- Référence CVE CVE-2009-0147 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0147>
- Référence CVE CVE-2009-0163 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0163>
- Référence CVE CVE-2009-0166 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0166>
- Référence CVE CVE-2009-0195 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0195>
- Référence CVE CVE-2009-0799 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0799>
- Référence CVE CVE-2009-0800 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0800>
- Référence CVE CVE-2009-1179 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1179>

- Référence CVE CVE-2009-1180 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1180>
- Référence CVE CVE-2009-1181 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1181>
- Référence CVE CVE-2009-1182 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1182>
- Référence CVE CVE-2009-1183 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1183>

## **Gestion détaillée du document**

**21 avril 2009** version initiale.

**11 mai 2009** ajout des références aux bulletins de sécurité Gentoo, Debian, RedHat et SuSE.