

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de Ghostscript

---

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-2002-AVI-129>

---

### Gestion du document

Référence	CERTA-2002-AVI-129
Titre	Vulnérabilité de Ghostscript
Date de la première version	14 juin 2002
Date de la dernière version	–
Source(s)	Bulletin de sécurité RHSA-2002-083 de RedHat
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.

## 2 Systèmes affectés

Logiciel Ghostscript sous Linux.

## 3 Résumé

Un utilisateur mal intentionné peut exécuter du code arbitraire avec les privilèges de l'utilisateur exécutant Ghostscript au moyen d'un document PostScript habilement conçu.

## 4 Description

Ghostscript est un interpréteur de document PostScript (extension de type `.ps`). Il est utilisé comme visionneur et comme filtre d'impression pour les documents PostScript.

Il est possible de construire un document PostScript permettant d'exécuter du code arbitraire avec les permissions de l'utilisateur qui exécute Ghostscript. Cette vulnérabilité est d'autant plus dangereuse qu'elle peut être exécutée par l'utilisateur `lp` qui possède plus de privilèges qu'un utilisateur standard.

## **5 Solution**

Consulter les bulletins de sécurité de votre distributeur pour connaître la disponibilité des correctifs.

## **6 Documentation**

Bulletin de sécurité RHSA-2002:083 de RedHat :  
<http://rhn.redhat.com/errata/RHSA-2002-083.html>

## **Gestion détaillée du document**

**14 juin 2002** version initiale.