



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 28 novembre 2005  
N° CERTA-2004-AVI-351-001

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans 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-2004-AVI-351>

---

### Gestion du document

Référence	CERTA-2004-AVI-351-001
Titre	Vulnérabilité dans Ghostscript
Date de la première version	21 octobre 2004
Date de la dernière version	28 novembre 2005
Source(s)	Bulletin de sécurité Gentoo GLSA-200410-18 du 20 octobre 2004
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 l'intégrité des données.

## 2 Systèmes affectés

Ghostscript 7.07.1-r7 et versions antérieures.

## 3 Résumé

Une vulnérabilité présente dans Ghostscript permet à un utilisateur local, mal intentionné, de porter atteinte à l'intégrité des données présentes sur le système.

## 4 Description

L'application Ghostscript est un interpréteur de fichier PostScript (PS) et PDF. Les scripts `pj-gs.sh`, `ps2epsi.sh`, `pv.sh` et `sysvlp.sh`, présents dans Ghostscript sont vulnérables à une attaque classique d'écrasement de fichiers via le suivi des liens symboliques. A l'aide de liens habilement constitués, un utilisateur mal intentionné, ayant un accès local au système, peut forcer la modification de fichiers avec les droits de la victime.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité Gentoo GLSA-200410-18 du 20 octobre 2004 :  
<http://www.gentoo.org/security/en/glsa/glsa-200410-18.xml>
- Bulletins de sécurité FreeBSD pour ghostscript-gnu, ghostscript-gnu-nox11, ghostscript-afpl et ghostscript-afpl-nox11 du 27 novembre 2005 :  
<http://www.vuxml.org/freebsd/pkg-ghostscript-gnu.html>  
<http://www.vuxml.org/freebsd/pkg-ghostscript-gnu-nox11.html>  
<http://www.vuxml.org/freebsd/pkg-ghostscript-afpl.html>  
<http://www.vuxml.org/freebsd/pkg-ghostscript-afpl-nox11.html>
- Référence CVE CAN-2004-0967 :  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0967>

## Gestion détaillée du document

**21 octobre 2004** version initiale.

**28 novembre 2005** ajout des références aux bulletins de sécurité FreeBSD.