



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 novembre 2005
N° CERTA-2005-AVI-472

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le logiciel FUSE

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-2005-AVI-472>

Gestion du document

Référence	CERTA-2005-AVI-472
Titre	Vulnérabilité dans le logiciel FUSE
Date de la première version	30 novembre 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité de FUSE
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

Élévation de privilèges.

2 Systèmes affectés

FUSE version 2.4.1 et versions antérieures.

3 Résumé

Une vulnérabilité a été découverte dans FUSE permettant d'élever ses privilèges en local sur un système vulnérable.

4 Description

FUSE est un outil permettant d'implémenter un système de fichier dans l'espace de travail d'un programme.

FUSE présente une vulnérabilité permettant à un utilisateur local mal intentionné de corrompre le fichier */etc/mtab*.

L'exploitation de cette vulnérabilité n'est possible que si le programme est installé avec le drapeau *suid root*.

5 Contournement provisoire

Retirer de l'application le drapeau *suid root*.

6 Solution

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

7 Documentation

- Bulletin de sécurité FUSE du 17 novembre 2005:
http://sourceforge.net/project/shownotes.php?release_id=373087
- Bulletin de sécurité Gentoo GLSA-200511-17 du 22 novembre 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200511-17.xml>
- Bulletin de sécurité Mandriva MDKSA-2005:216 du 24 novembre 2005 :
<http://frontal2.mandriva.com/security/advisories?name=MDKSA-2005:216>
- Référence CVE CVE-2005-3531 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3531>

Gestion détaillée du document

30 novembre 2005 version initiale.