

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités de grsecurity

---

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-106>

---

### Gestion du document

Référence	CERTA-2005-AVI-106
Titre	Multiples vulnérabilités de grsecurity
Date de la première version	11 mars 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité grsecurity du 07 mars 2005
Pièce(s) jointe(s)	

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

## 1 Risque

Elévation de privilèges ;

## 2 Systèmes affectés

grsecurity 2.1.2 et versions antérieures.

## 3 Résumé

Deux vulnérabilités découvertes dans grsecurity permettent à un utilisateur mal intentionné d'élever ses privilèges sur le système vulnérable.

## 4 Description

grsecurity est une suite de correctifs de sécurité destinée à augmenter la sécurité du système fonctionnant sous Linux.

- une vulnérabilité existante dans les versions antérieures à grsecurity 2.1.2 permet à un utilisateur mal intentionné ayant un accès local au système d'élever ses privilèges. Cette vulnérabilité n'est pas exploitable si grsecurity est configuré avec un niveau de sécurité *LOW* ou *MEDIUM* ;
- la seconde vulnérabilité présente dans le système RBAC (Role-Based Access Control) permet à un individu local mal intentionné d'élever ses privilèges.

## **5 Solution**

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

## **6 Documentation**

- Bulletin de sécurité grsecurity du 07 mars 2005 :  
<http://www.grsecurity.org/news.php#grsec213>

## **Gestion détaillée du document**

**11 mars 2005** version initiale.