

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de la commande `sudo`

---

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-065>

---

### Gestion du document

Référence	CERTA-2009-AVI-065
Titre	Vulnérabilité de la commande <code>sudo</code>
Date de la première version	12 février 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité courtesan du 29 janvier 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

- Élévation de privilèges ;
- contournement de la politique de sécurité.

## 2 Systèmes affectés

`sudo` versions inférieures à la version 1.6.9p19.

## 3 Résumé

Une vulnérabilité de la commande `sudo` permet à un utilisateur malintentionné d'élever ses privilèges ou de contourner la politique de sécurité mise en place.

## 4 Description

Une vulnérabilité a été découverte dans la commande `sudo`, sous certaines conditions de configuration. L'exploitation de cette vulnérabilité permet de contourner la politique de sécurité intrinsèque à cette commande, voire 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 de courtesan du 29 janvier 2009 :  
[http://www.courtesan.com/sudo/alerts/group\\_vector.html](http://www.courtesan.com/sudo/alerts/group_vector.html)
- Bulletin de sécurité Mandriva du 04 février 2009 :  
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:033>
- Bulletin de mise à jour gentoo linux du 06 février 2009 :  
<http://www.gentoo.org/security/en/glsa/glsa-200902-01.xml>
- Référence CVE CVE-2009-0034 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0034>

## Gestion détaillée du document

**12 février 2009** version initiale.