

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans 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-2011-AVI-013>

Gestion du document

Référence	CERTA-2011-AVI-013-001
Titre	Vulnérabilité dans sudo
Date de la première version	14 janvier 2011
Date de la dernière version	07 mars 2012
Source(s)	Bulletin de sécurité sudo du 12 janvier 2011
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

sudo 1.7.0 à 1.7.4p4.

3 Résumé

Une vulnérabilité dans la commande *sudo* permet à un utilisateur malveillant d'élever ses privilèges.

4 Description

La commande *sudo* a été enrichie d'une fonction de changement de groupe lors du passage à la version 1.7.0. Dans certaines configurations, un utilisateur malveillant peut acquérir sans vérification les droits assignés à un groupe dont il n'est pas membre.

5 Solution

La version 1.7.4p5 remédie à ce problème.

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

6 Documentation

- Bulletin de sécurité sudo du 12 janvier 2011 :
http://www.sudo.ws/sudo/alerts/runas_group_pw.html
- Bulletin de sécurité Gentoo GLSA 201203-06 du 06 mars 2012 :
<http://www.gentoo.org/security/en/glsa/glsa-201203-06.xml>
- Référence CVE CVE-2011-0010 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0010>

Gestion détaillée du document

14 janvier 2011 version initiale.

07 mars 2012 ajout du bulletin de sécurité Gentoo.