

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de 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-2005-AVI-495>

Gestion du document

Référence	CERTA-2005-AVI-495-002
Titre	Vulnérabilité de Sudo
Date de la première version	21 décembre 2005
Date de la dernière version	23 janvier 2006
Source(s)	Bulletin de sécurité Mandriva MDKSA-2005:234 du 20 décembre 2005
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

Exécution de commandes arbitraires par des utilisateurs locaux.

2 Systèmes affectés

Toutes les versions de sudo antérieures à la version 1.6.8p12.

3 Description

L'utilitaire sudo permet d'accorder des droits d'administration à des utilisateurs non privilégiés du système. Une vulnérabilité de sudo dans la gestion des variables d'environnement PERLLIB, PERL5LIB et PERL5OPT permet à un utilisateur local d'exécuter des commandes arbitraires.

4 Solution

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

5 Documentation

- Site Internet de sudo :
<http://www.sudo.ws>
- Bulletin de sécurité sudo :
http://www.sudo.ws/sudo/alerts/perl_env.html
- Bulletin de sécurité Mandriva MDKSA-2005:234 du 20 décembre 2005 :
<http://frontal2.mandriva.com/security/advisories?name=MDKSA-2005:234>
- Bulletin de sécurité Debian DSA-946 du 20 janvier 2006 :
<http://www.debian.org/security/2006/dsa-946>
- Bulletin de sécurité SUSE SUSE-SR:2006:002 du 20 janvier 2006 :
http://www.novell.com/linux/security/advisories/2006o_02_sr.html
- Référence CVE CAN-2005-4158 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-4158>

Gestion détaillée du document

21 décembre 2005 version initiale.

20 janvier 2006 ajout de la référence au bulletin de sécurité Debian.

23 janvier 2006 ajout de la référence au bulletin de sécurité SUSE.