



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 24 novembre 2004
N° CERTA-2004-AVI-371-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans l'utilitaire 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-2004-AVI-371>

Gestion du document

Référence	CERTA-2004-AVI-371-002
Titre	Vulnérabilité dans l'utilitaire sudo
Date de la première version	19 novembre 2004
Date de la dernière version	24 novembre 2004
Source(s)	Bulletin de sécurité sudo
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

Elévation de privilèges.

2 Systèmes affectés

Versions de sudo antérieures à la version 1.6.8p2.

3 Résumé

sudo est un utilitaire qui permet d'accorder des droits d'administration à des utilisateurs non privilégiés du système. Une vulnérabilité dans l'utilisation de variables d'environnement par sudo permet à un utilisateur local mal intentionné d'exécuter du code arbitraire afin d'élever ses privilèges.

4 Solution

Mettre à jour l'utilitaire sudo avec la version 1.6.8p2 disponible sur le site suivant :
<http://www.sudo.ws>

5 Documentation

- Bulletin de sécurité sudo :
http://www.sudo.ws/sudo/alerts/bash_functions.html
- Bulletin de sécurité Mandrake MDKSA-2004:133 du 15 novembre 2004 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:133>
- Bulletin de sécurité FreeBSD pour sudo du 11 novembre 2004 :
<http://www.vuxml.org/freebsd/>
- Mise à jour de sécurité du paquetage NetBSD sudo :
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/security/sudo/README.html>
- Bulletin de sécurité Debian DSA-596 du 24 novembre 2004 :
<http://www.debian.org/security/2004/dsa-596>
- Référence CVE CAN-2004-1051 :
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1051>

Gestion détaillée du document

19 novembre 2004 version initiale.

22 novembre 2004 ajout des références aux bulletins de sécurité Mandrake, FreeBSD et NetBSD.

24 novembre 2004 ajout de la référence au bulletin de sécurité Debian.