

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-2002-AVI-006>

Gestion du document

Référence	CERTA-2002-AVI-006
Titre	Vulnérabilité dans Sudo
Date de la première version	16 janvier 2002
Date de la dernière version	–
Source(s)	Avis de sécurité SuSE:2002:002
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

Version de sudo antérieure à la version 1.6.4.

3 Résumé

sudo est un utilitaire qui permet d'accorder des droits d'administration à des utilisateurs non privilégiés du système.

Une vulnérabilité présente dans sudo permet à un utilisateur mal intentionné de prendre les droits du super-utilisateur sur la machine.

4 Description

`sudo` utilise le logiciel de messagerie avec les privilèges du compte `root` et des variables d'environnement non sûres.

En forçant l'envoi de journaux de connexions par méls, un utilisateur mal intentionné peut exploiter cette vulnérabilité pour réaliser une élévation de privilèges.

Cette vulnérabilité n'est exploitable qu'en local.

5 Contournement provisoire

Retirer le `setuserid` bit du fichier `sudo` dans le répertoire `/usr/bin/` en attendant d'appliquer les correctifs.

6 Solution

Installer la versions 1.6.4 disponible sur le site <http://www.sudo.ws/sudo>

Des mises à jour sont également disponibles sous forme de paquetages pour les distributions Linux (cf. section Documentation).

7 Documentation

- Avis de sécurité DSA-101 de Debian :
<http://www.debian.org/security/2002/dsa-101>
- Avis de sécurité SuSE-SA:2002:002 de SuSE :
<http://www.suse.com/us/support/security>
- Avis de sécurité RHSA-2002:011 de RedHat :
<http://www.redhat.com/support/errata/RHSA-2002-011.html>
- Avis de sécurité MDKSA-2002:003 de Mandrake :
<http://www.mandrakesecure.net/en/advisories/2002/MDKSA-2002-003.php>

Gestion détaillée du document

16 janvier 2002 version initiale.