

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-2010-AVI-299>

Gestion du document

Référence	CERTA-2010-AVI-299
Titre	Vulnérabilité de sudo
Date de la première version	02 juillet 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité du projet 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

Élévation de privilèges.

2 Systèmes affectés

sudo, version 1.x.

3 Résumé

Une vulnérabilité de *sudo* permet à un utilisateur malveillant d'élever ses privilèges.

4 Description

Lorsque le programme *sudo* est utilisé avec l'option `secure path`, un utilisateur malveillant peut exécuter des commandes qui ne lui sont pas autorisées en manipulant la variable `PATH`.

5 Solution

Les version 1.6.9p23 et 1.7.2p7 remédient à ce problème.

Se référer aux bulletins de sécurité des éditeurs pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité du projet sudo :
http://www.sudo.ws/sudo/alerts/secure_path.html
- Bulletin de sécurité Debian DSA 2062 du 17 juin 2010 :
<http://www.debian.org/security/2010/dsa-2062>
- Mise à jour de sécurité Fedora FEDORA-2010-9402 du 14 juin 2010 :
<http://lists.fedoraproject.org/pipermail/package-announce/2010-June/042838.html>
- Mise à jour de sécurité Fedora FEDORA-2010-9415 du 21 juin 2010 :
<http://lists.fedoraproject.org/pipermail/package-announce/2010-June/043026.html>
- Mise à jour de sécurité Fedora FEDORA-2010-9417 du 21 juin 2010 :
<http://lists.fedoraproject.org/pipermail/package-announce/2010-June/043012.html>
- Bulletin de sécurité Mandriva MDVSA-2010:118 du 17 juin 2010 :
<http://www.mandriva.com/security/advisories?name=MDVSA-2010:118>
- Bulletin de sécurité RedHat RHSA-2010:0475 du 15 juin 2010 :
<http://rhn.redhat.com/errata/RHSA-2010-0475.html>
- Bulletin de sécurité Ubuntu USN-956-1 du 30 juin 2010 :
<http://www.ubuntulinux.org/usn/usn-956-1>
- Référence CVE CVE-2010-1646 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1646>

Gestion détaillée du document

02 juillet 2010 version initiale.