

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans OpenSSH

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-308>

Gestion du document

Référence	CERTA-2004-AVI-308-003
Titre	Vulnérabilité dans OpenSSH
Date de la première version	09 septembre 2004
Date de la dernière version	31 août 2005
Source(s)	Bulletin de sécurité SUSE du 14 Avril 2004
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

Atteinte à l'intégrité des données.

2 Systèmes affectés

OpenSSH versions antérieures à 3.4p1.

3 Description

Une vulnérabilité est présente dans l'utilitaire SCP d'OpenSSH. Cette vulnérabilité peut être employée par un utilisateur mal intentionné afin d'écraser des fichiers existants sur le système client, lors de l'utilisation de SCP sur un serveur OpenSSH malicieux.

4 Solution

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

5 Documentation

- Bulletin de sécurité SUSE du 14 Avril 2004 :
http://www.suse.de/de/security/2004_09_kernel.html
- Bulletin de sécurité #59739 de Juniper Networks NetScreen :
<http://www.juniper.net/support/security/alerts/adv59739.txt>
- Bulletin de sécurité MAC OS X du 07 Septembre 2004 :
<http://docs.info.apple.com/article.html?artnum=61798>
- Bulletin de sécurité Red Hat RHSA-2005:106 du 18 mai 2005 :
<https://rhn.redhat.com/errata/RHSA-2005-106.html>
- Bulletin de sécurité Red Hat RHSA-2005:165 du 06 juin 2005 :
<https://rhn.redhat.com/errata/RHSA-2005-165.html>
- Bulletin de sécurité Red Hat RHSA-2005:495 du 13 juin 2005 :
<https://rhn.redhat.com/errata/RHSA-2005-495.html>
- Bulletin de sécurité Mandriva MDKSA-2005:100 du 14 juin 2005 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2005:100>
- Bulletin de sécurité Avaya ASA-2005-167 du 29 août 2005 :
<http://support.avaya.com/elmodocs2/security/ASA-2005-167.pdf>
- Référence CVE CAN-2004-0175 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0175>

Gestion détaillée du document

09 septembre 2004 version initiale.

09 juin 2005 ajout références aux bulletins RHSA-2005-106 et RHSA-2005-165 de Red Hat.

15 juin 2005 ajout références aux bulletins de sécurité RHSA-2005-495 de Red Hat et MDKSA-2005:100 de Mandriva.

31 août 2005 ajout référence au bulletin de sécurité ASA-2005-167 de Avaya.