Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 mai 2008
N° CERTA-2008-AVI-246

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans OpenSSH pour Debian et Ubuntu

Gestion du document

Référence	CERTA-2008-AVI-246
Titre	Vulnérabilité dans OpenSSH pour Debian et Ubuntu
Date de la première version	15 mai 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Debian DSA-1576 du 14 mai 2008
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

- Contournement de la politique de sécurité ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- la version de OpenSSH mise en œuvre dans Debian Etch ;
- la version de OpenSSH mise en œuvre dans les versions 7.04, 7.10 et 8.04 de Ubuntu.

La version présente dans l'ancienne version stable de Debian : *sarge* n'est pas vulnérable.

3 Résumé

Une vulnérabilité dans la version de OpenSSH propre aux distributions Debian, Ubuntu ou à leurs dérivés permet à un utilisateur distant de contourner la politique de sécurité ou de porter atteinte à la confidentialité du système vulnérable.

4 Description

Par effet de bord, la vulnérabilité décrite dans l'avis CERTA-2008-AVI-239 sur `OpenSSL`, s'applique également au paquetage `OpenSSH` des distributions `Debian` et `Ubuntu`. Tous les bi-clefs `ssh` engendrés par la commande *ssh-keygen* fournie par les versions vulnérables de `OpenSSH` sont donc considérés comme non-fiables et doivent être renouvelés.

5 Solution

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

6 Documentation

- Bulletin de sécurité Debian DSA 1576 du 14 mai 2008 :
  http://www.debian.org/security/2008/dsa-1576
- Bulletin de sécurité Ubuntu USN-612-5 du 14 mai 2008 :
  http://www.ubuntulinux.org/usn/usn-612-5
- Référence CVE CVE-2008-0166 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0166

Gestion détaillée du document

15 mai 2008 version initiale.