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-239-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans la version OpenSSL de Debian

Gestion du document

Référence	CERTA-2008-AVI-239-001
Titre	Vulnérabilité dans la version OpenSSL de Debian
Date de la première version	13 mai 2008
Date de la dernière version	15 mai 2008
Source(s)	Bulletin de sécurité DSA-1571 du 13 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

- OpenSSL pour Debian versions 0.9.8c-4etch2 et antérieures ;
- les versions d'OpenSSL mises 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 `OpenSSL` 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

Une vulnérabilité est présente dans la version spécifique de OpenSSL mise en œuvre dans les distributions GNU/Linux Debian et Ubuntu. Celle-ci est relative à une faiblesse dans le générateur de nombres pseudo-aléatoires. Cette faille permet potentiellement à un utilisateur malintentionné de prédire les clefs engendrées au moyen de OpenSSL.

Remarque : les clefs créées avec la version vulnérable d'OpenSSL sont donc considérées comme non-fiables et doivent être remplacées par de nouvelles après application du correctif.

5 Solution

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

6 Documentation

- Bulletin de sécurité Debian DSA 1571 du 13 mai 2008 :
  http://www.debian.org/security/2008/dsa-1571
- Bulletin de sécurité Ubuntu USN-612-1 du 13 mai 2008 :
  http://www.ubuntu.com/usn/usn-612-1

Gestion détaillée du document

13 mai 2008 version initiale ;
15 mai 2008 ajout de Ubuntu dans les systèmes vulnérables, ajout de la non-vulnérabilité de la Debian sarge.