

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans OpenSSL

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-385>

Gestion du document

Référence	CERTA-2004-AVI-385-002
Titre	Vulnérabilité dans OpenSSL
Date de la première version	02 décembre 2004
Date de la dernière version	31 août 2005
Source(s)	Avis de sécurité Debian DSA-603 du 01 décembre 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

Elévation de privilèges.

2 Systèmes affectés

OpenSSL versions 0.9.6m, 0.9.7d et 0.9.7e.

3 Résumé

Une vulnérabilité a été découverte dans certaines versions d'OpenSSL, permettant à un utilisateur local mal intentionné d'élever ses privilèges.

4 Description

Une vulnérabilité présente dans le script `der_chop` permet à un utilisateur local mal intentionné, en utilisant un lien symbolique, de créer ou d'écraser certains fichiers temporaires avec les privilèges de l'utilisateur ayant lancé le script.

5 Solution

Appliquer le correctif corrigeant cette faille suivant la distribution affectée (cf. Documentation).

6 Documentation

- Bulletin de sécurité Debian DSA-603 du 01 décembre 2004 :
<http://www.debian.org/security/2004/dsa-603>
- Bulletin de sécurité Gentoo GLSA-200411-15 du 08 Novembre 2004 :
<http://security.gentoo.org/glsa/glsa-200411-15.xml>
- Bulletin de sécurité Mandrake MDKSA-2004:147 du 06 décembre 2004 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:147>
- Bulletin de sécurité Avaya ASA-2005-170 du 29 août 2005 :
<http://support.avaya.com/elmodocs2/security/ASA-2005-170.pdf>
- Référence CVE CAN-2004-0975 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0975>

Gestion détaillée du document

02 décembre 2004 version initiale.

06 décembre 2004 ajout de la référence au bulletin de sécurité Mandrake.

31 août 2004 ajout de la référence au bulletin de sécurité Avaya.