Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 août 2007
N° CERTA-2007-AVI-313-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans la bibliothèque libarchive

Gestion du document

Référence	CERTA-2007-AVI-313-001
Titre	Vulnérabilité dans la bibliothèque libarchive
Date de la première version	18 juillet 2007
Date de la dernière version	08 août 2007
Source(s)	Bulletin de sécurité FreeBSD du 12 juillet 2007
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

- Exécution de code arbitraire à distance ;
- déni de service.

2 Systèmes affectés

- libarchive 1.x ;
- libarchive 2.x.

3 Résumé

Une vulnérabilité dans la vulnérabilité `libarchive` permet à un utilisateur distant de provoquer un déni de service ou potentiellement d'exécuter du code arbitraire.

4 Description

Une vulnérabilité dans la bibliothèque de fonctions `libarchive` a été identifiée. Cette bibliothèque est, en particulier, utilisée par la commande d'archivage `tar`. Un utilisateur distant malintentionné peut ainsi provoquer

un arrêt de l'application vulnérable ou exécuter du code arbitraire via une archive de type `tar` particulière.
NB : un simple listage (`tar -t`) de l'archive suffit pour exploiter la vulnérabilité.

5 Solution

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

6 Documentation

- Bulletin de sécurité FreeBSD SA-07:05.libarchive du 12 juillet 2007 :
  ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-07:05.libarchive.asc
- Bulletin de sécurité Gentoo GLSA-200708-03 du 08 août 2007 :
  http://www.gentoo.org/security/en/glsa/glsa-200708-03.xml
- Bulletin de sécurité SuSE SUSE-SR:2007:015 du 03 août 2007 :
  http://lists.opensuse.org/opensuse-security-announce/2007-08/msg00003.htm
- Référence CVE CVE-2007-3641 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3641
- Référence CVE CVE-2007-3644 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3644
- Référence CVE CVE-2007-3645 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3645

Gestion détaillée du document

18 juillet 2007 version initiale.

08 août 2007 modification des systèmes affectés, ajout des références CVE et des références aux bulletins de sécurité Gentoo et SuSE.