Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 25 janvier 2007
N° CERTA-2006-AVI-516-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de GNU tar

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-2006-AVI-516

Gestion du document

Référence	CERTA-2006-AVI-516-002
Titre	Vulnérabilité de GNU tar
Date de la première version	29 novembre 2006
Date de la dernière version	25 janvier 2007
Source(s)	
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

Distributions intégrant *GNU tar version 1.16, 1.15.1* et probablement des versions antérieures.

3 Résumé

Un attaquant peut écrire ou écraser des fichiers existants à l'aide d'une archive au format `tar`.

4 Description

Un attaquant peut construire une archive `tar` malveillante avec un lien symbolique qui n'est pas correctement traité par les fonctions `extract_archive` du fichier source `extract.c` et `extract_mangle` du fichier source`mangle.c`. L'attaquant pourra écrire ou écraser des fichiers à un endroit arbitraire sur le système vulnérable, dans le contexte de l'utilisateur qui manipulera cette archive.

Un code prouvant la faisabilité de l'attaque circule sur l'Internet.

5 Solution

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

6 Documentation

- Bulletin de sécurité Mandriva MDKSA-2006:219 du 28 novembre 2006 :
  http://www.mandriva.com/security/advisories?name=MDKSA-2006:219
- Bulletin de sécurité Ubuntu USN-385-1 du 27 novembre 2006 :
  http://www.ubuntu.com/usn/usn-385-1
- Bulletin de sécurité Red Hat RHSA-2006:0749 du 19 décembre 2006 :
  http://rhn.redhat.com/errata/RHSA-2006-0749.html
- Bulletin de sécurité Gentoo GLSA-200612-10 du 11 décembre 2006 :
  http://www.gentoo.org/security/en/glsa/glsa-200612-10.xml
- Bulletin de sécurité Debian DSA-1223 du 01 décembre 2006 :
  http://www.debian.org/security/2006/dsa-1223
- Bulletin de sécurité FreeBSD SA-06:26 du 06 décembre 2006 :
  http://security.freebsd.org/advisories/FreeBSD-SA-06:26.gtar.asc
- Référence CVE CVE-2006-6097 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6097
- Bulletin de sécurité Avaya ASA-2007-015 du 24 janvier 2007 :
  http://support.avaya.com/elmodocs2/security/ASA-2007-015.htm

Gestion détaillée du document

29 novembre 2006 version initiale.

20 décembre 2006 ajout des références aux bulletins de sécurité Red Hat, Gentoo, Debian, FreeBSD.

25 janvier 2007 ajout du bulletin de sécurité concernant les produits Avaya.