Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 07 décembre 2009
N° CERTA-2007-AVI-377-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans GNU tar

Gestion du document

Référence	CERTA-2007-AVI-377-002
Titre	Vulnérabilité dans GNU tar
Date de la première version	24 août 2007
Date de la dernière version	07 décembre 2009
Source(s)	Bulletin de sécurité Redhat RHSA-2007:0860 du 23 août 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

Contournement de la politique de sécurité.

2 Systèmes affectés

- GNU tar versions antérieures à 1.18 ;
- Solaris 9 sur SPARC ;
- Solaris 10 sur SPARC sans le patch 139099-03 ;
- OpenSolaris sur SPARC de svn_01 à svn _115 ;
- Solaris 9 sur x86 ;
- Solaris 10 sur x86 sans le patch 139100-03 ;
- OpenSolaris sur x86 de svn_01 à svn_11.

3 Résumé

Une vulnérabilité de `GNU tar` permet de contourner la politique de sécurité.

4 Description

Un manque de vérification de certains attributs d'une archive `tar` permet à un utilisateur malveillant d'extraire des fichiers ou des dossiers contenus dans l'archive vers des emplacements arbitraires. Un utilisateur exploitant cette vulnérabilité peut contourner la politique de sécurité en créant ou en écrasant des données sensibles.

5 Solution

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

6 Documentation

- Bulletin de sécurité Gentoo GLSA-200709-09 du 15 septembre 2007 :
  http://www.gentoo.org/security/en/glsa/glsa-200709-09.xml
- Bulletin de sécurité Debian DSA-1438 du 28 décembre 2008 :
  http://www.debian.org/security/2008/dsa-1438
- Bulletin de sécurité RedHat RHSA-2007:0860 du 23 août 2007 :
  http://rhn.redhat.com/errata/RHSA-2007-0860.html
- Bulletin de sécurité Mandriva MDKSA-2007:173 du 4 septembre 2007 :
  http://www.mandriva.com/security/advisories?name=MDKSA-2007:173
- Bulletin de sécurité SuSE SUSE-SA:2007:018 du 31 août 2007 :
  http://www.novell.com/linux/security/advisories/2007_18_sr.html
- Bulletin de sécurité Ubuntu USN-506-1 du 28 août 2007 :
  http://www.ubuntu.com/usn/usn-506-1
- Bulletin de sécurité FreeBSD FreeBSD-SA-07:10.gtar du 29 novembre 2007 :
  http://security.freebsd.org/advisories/FreeBSD-SA-07:10.gtar.asc
- Bulletin de sécurité Avaya ASA-2007-383 du 26 septembre 2007 :
  http://support.avaya.com/elmodocs2/security/ASA-2007-383.htm
- Référence CVE CVE-2007-4131 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4131
- Bulletin de sécurité Sun 1-66-273551-1 du 2 décembre 2009 :
  http://sunsolve.sun.com/search/document.do?assetkey=1-66-273551-1

Gestion détaillée du document

24 août 2007 version initiale.

07 octobre 2008 ajout des références aux bulletins de sécurité Gentoo, Debian, Mandriva, SuSE, Ubuntu, FreeBSD et Avaya.

07 décembre 2009 ajout des références au bulletin de sécurité Sun 1-66-273551-1 du 02 décembre 2009.