

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans 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-2007-AVI-391>

Gestion du document

Référence	CERTA-2007-AVI-391-004
Titre	Vulnérabilité dans GNU Tar
Date de la première version	06 septembre 2007
Date de la dernière version	04 décembre 2009
Source(s)	Bulletin de sécurité SuSE SUSE-SR:2007:018 du 31 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

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

2 Systèmes affectés

- GNU tar ;
- Solaris 9 sur SPARC ;
- Solaris 10 sur SPARC sans le patch 139099-03 ;
- OpenSolaris sur SPARC de snv_01 à snv_115 ;
- Solaris 9 sur x86 ;
- Solaris 10 sur x86 sans le patch 139100-03 ;
- OpenSolaris sur x86 de snv_01 à snv_11.

3 Description

Une vulnérabilité a été identifiée dans GNU tar. L'exploitation d'un débordement de mémoire dans la fonction `safer_name_suffix()` peut compromettre la pile. L'impact est inconnu.

4 Solution

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

5 Documentation

- Bulletin de sécurité Gentoo GLSA-200711-18 du 14 novembre 2007 :
<http://www.gentoo.org/security/en/glsa/glsa-200711-18.xml>
- Bulletin de sécurité Debian DSA-1566 du 02 mai 2008 :
<http://www.debian.org/security/2008/dsa-1566>
- Bulletin de sécurité Debian DSA-1438 du 28 décembre 2008 :
<http://www.debian.org/security/2008/dsa-1438>
- Bulletin de sécurité Mandriva MDVSA-2007:233 du 28 novembre 2007 :
<http://www.mandriva.com/en/security/advisories?name=MDKSA-2007-233>
- Bulletin de sécurité Ubuntu USN-650-1 du 02 octobre 2008 :
<http://www.ubuntu.com/usn/usn-650-1>
- 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 SuSE SUSE-SA:2007:019 du 28 septembre 2007 :
http://www.novell.com/linux/security/advisories/2007_19_sr.html
- Référence CVE CVE-2007-4476 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4476>
- Bulletin de sécurité Sun 1-66-273551-1 du 02 décembre 2009 :
<http://sunsolve.sun.com/search/document.do?assetkey=1-66-273551-1>

Gestion détaillée du document

06 septembre 2007 version initiale.

07 novembre 2007 ajout de la référence au bulletin de sécurité SuSE.

30 novembre 2007 ajout de la référence au bulletin de sécurité Mandriva.

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

04 décembre 2009 ajout des références aux bulletins de sécurité Sun et des systèmes affectés.