



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 18 octobre 2007
N° CERTA-2005-AVI-188-006

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans bzip2

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-2005-AVI-188>

Gestion du document

Référence	CERTA-2005-AVI-188-006
Titre	Multiples vulnérabilités dans bzip2
Date de la première version	02 juin 2005
Date de la dernière version	18 octobre 2007
Source(s)	Mise à jour de sécurité de l'éditeur du 26 mai 2005
Pièce(s) jointe(s)	

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Déni de service ;
- atteinte à la confidentialité des données ;
- atteinte à l'intégrité des données.

2 Systèmes affectés

bzip2 1.x.

3 Description

bzip2 est un outil de compression.

- Une première vulnérabilité permet à un individu malintentionné de porter atteinte à la confidentialité et à l'intégrité des données au moyen de liens symboliques contenus dans une archive spécialement construite (CAN-2005-0953) ;
- une seconde vulnérabilité présente dans l'application bzip2 permet à un utilisateur distant malintentionné, au moyen d'une archive spécialement construite, de consommer une grande partie des ressources CPU du système afin de réaliser un déni de service (CAN-2005-1260).

4 Solution

Se référer aux bulletins de sécurité des éditeurs pour l'obtention des correctifs (cf. section Documentation). Appliquer la mise à jour de sécurité de l'éditeur disponible à l'adresse suivante : <http://www.bzip.org/downloads.html>

5 Documentation

- Site Internet de l'éditeur : <http://www.bzip.org>
- Mise à jour de sécurité bzip2 v1.0.3 : <http://www.bzip.org/downloads.html>
- Bulletin de sécurité Debian DSA-730 du 27 mai 2005 : <http://www.debian.org/security/2005/dsa-730>
- Bulletin de sécurité Mandriva MDKSA-2005:091 du 18 mai 2005 : <http://www.mandriva.com/security/advisories?name=MDKSA-2005:091>
- Bulletin de sécurité SUSE SUSE-SR:2005:015 du 07 juin 2005 : http://www.novell.com/linux/security/advisories/2005_15_sr.html
- Bulletin de sécurité RedHat RHSA-2005:474 du 16 juin 2005 : <http://rhn.redhat.com/errata/RHSA-2005-474.html>
- Bulletin de sécurité FreeBSD du 29 juin 2005 : <ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:14.bzip2.asc>
- Bulletin de sécurité Debian DSA-741 du 07 juillet 2005 : <http://www.debian.org/security/2005/dsa-741>
- Bulletin de sécurité Sun 103118 du 16 octobre 2007 : <http://sunsolve.sun.com/search/document.do?assetkey=1-26-103118-1>
- Référence CVE CAN-2005-0953 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0953>
- Référence CVE CAN-2005-1260 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1260>

Gestion détaillée du document

02 juin 2005 version initiale.

03 juin 2005 ajout d'une nouvelle vulnérabilité, de la référence CVE et des références aux bulletins de sécurité Mandriva et Debian.

14 juin 2005 ajout de la référence au bulletin de sécurité SUSE SUSE-SR:2005:015.

17 juin 2005 ajout de la référence au bulletin de sécurité RedHat RHSA-2005:474.

01 juillet 2005 ajout de la référence au bulletin de sécurité FreeBSD SA-05:14.

07 juillet 2005 ajout de la référence au bulletin de sécurité Debian DSA-741.

18 octobre 2007 ajout de la référence au bulletin de sécurité Sun 103118.