Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 29 novembre 2010
N° CERTA-2010-AVI-449-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans bzip2

Gestion du document

Référence	CERTA-2010-AVI-449-001
Titre	Vulnérabilité dans bzip2
Date de la première version	22 septembre 2010
Date de la dernière version	29 novembre 2010
Source(s)	Annonce du projet bzip du 20 septembre 2010
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

Déni de service à distance.

2 Systèmes affectés

bzip2, version 1.0.5 et versions précédentes.
Les logiciels utilisant le code vulnérable sont concernés (liste non exhaustive) :
– Clamav, version 0.96.2 et versions précédentes ;
– FreeBSD, branches 6, 7 et8.

3 Résumé

Une vulnérabilité dans bzip2 permet à un utilisateur malveillant de provoquer un déni de service à distance.

4 Description

Un débordement d'entier dans la fonction de décompression est exploitable par un utilisateur malveillant pour provoquer un déni de service à distance par la soumission d'un fichier compressé spécialement conçu.

La possibilité d'exécuter du code arbitraire à distance est suspectée, mais non démontrée.

5 Solution

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

6 Documentation

- Annonce du projet bzip du 20 septembre 2010 :
  http://www.bzip.org/index.html
- Changements dans la version ClamAV 0.96.3 du 20 septembre 2010 :
  http://git.clamav.net/gitweb?p=clamav-devel.git;a=blob_plain;f=ChangeLog;hb=clamav-0.96.3
- Bulletin de sécurité Debian DSA-2112-1 du 20 septembre 2010 :
  http://www.debian.org/security/2010/dsa-2112
- Bulletin de sécurité FreeBSD-SA-10:08 du 20 septembre 2010 :
  http://security.freebsd.org/advisories/FreeBSD-SA-10:08.bzip2.asc
- Bulletin de sécurité RedHat RHSA-2010:0703-1 du 20 septembre 2010 :
  http://rhn.redhat.com/errata/RHSA-2010-0703.html
- Bulletin de sécurité Sun du 26 novembre 2010 :
  http://blogs.sun.com/security/entry/cve_2010_0405_integer_overflow
- Bulletin de sécurité SUSE SUSE-SA:2010:018 du 06 octobre 2010 :
  http://lists.opensuse.org/opensuse-security-announce/2010-10/msg00000.html
- Bulletin de sécurité Ubuntu USN-986-1 du 20 septembre 2010 :
  http://www.ubuntu.com/usn/usn-986-1
- Bulletin de sécurité Ubuntu USN-986-2 du 20 septembre 2010 :
  http://www.ubuntu.com/usn/usn-986-2
- Bulletin de sécurité Ubuntu USN-986-3 du 20 septembre 2010 :
  http://www.ubuntu.com/usn/usn-986-3
- Référence CVE CVE-2010-0405 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0405

Gestion détaillée du document

22 septembre 2010 version initiale.
29 novembre 2010 ajout des bulletins des distibutions Debian, RedHat, Sun, Suse et Ubuntu.