



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 décembre 2011
N° CERTA-2011-AVI-711

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans bzexe

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-2011-AVI-711>

Gestion du document

Référence	CERTA-2011-AVI-711
Titre	Vulnérabilité dans bzexe
Date de la première version	21 décembre 2011
Date de la dernière version	–
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

Élévation de privilèges.

2 Systèmes affectés

- Paquet bzip2 version inférieures à 1.0.5-6ubuntu1.11.10.1 pour système Ubuntu 11.10 ;
- Paquet bzip2 version inférieures à 1.0.5-6ubuntu1.11.04.1 pour système Ubuntu 11.04 ;
- Paquet bzip2 version inférieures à 1.0.5-4ubuntu1.1 pour système Ubuntu 10.10 ;
- Paquet bzip2 version inférieures à 1.0.5-4ubuntu0.2 pour système Ubuntu 10.04 LTS ;
- Paquet bzip2 version inférieures à 1.0.4-2ubuntu4.2 pour système Ubuntu 8.04 LTS.

3 Résumé

Une vulnérabilité dans le binaire *bzexe* inclus dans le paquet *bzip2* permet à un utilisateur local d'élever ses privilèges.

4 Description

L'exécutable *bzexe* permet de compresser des exécutables « en ligne ». Une faille dans la création des fichiers temporaires lors de cette compression permet à un attaquant local d'élever ses privilèges en exploitant une situation de concurrence (« *race condition* »).

5 Solution

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

6 Documentation

- Bulletin de sécurité Ubuntu USN-1308-1 du 14 décembre 2011 :
<http://www.ubuntu.com/usn/usn-1308-1/>
- Référence CVE CVE-2011-4089 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4089>

Gestion détaillée du document

21 décembre 2011 version initiale.