

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans la librairie `zlib` / `libz`

---

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-2002-AVI-052>

---

## Gestion du document

Référence	CERTA-2002-AVI-052
Titre	Vulnérabilité dans la librairie <code>zlib</code> / <code>libz</code>
Date de la première version	12 mars 2002
Date de la dernière version	–
Source(s)	Bulletin de sécurité SA:2002:010 de SuSE
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 ;
- deni de service.

## 2 Systèmes affectés

Les versions de la bibliothèque `zlib` / `libz` antérieures à la 1.1.4.

## 3 Résumé

Une vulnérabilité de type « débordement de mémoire » présente dans la librairie `zlib` / `libz` permet à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire en local ou à distance.

## 4 Description

La librairie `zlib` / `libz` est utilisée pour la compression et la décompression de données par un grand nombre d'applications.

Un débordement de mémoire présent dans la routine de décompression permet à un utilisateur mal intentionné d'exécuter du code arbitraire ou de réaliser un déni de service. Cette vulnérabilité est due à un double appel de la fonction de libération de la mémoire : la fonction `free`.

Beaucoup d'applications utilisent cette bibliothèque « dynamiquement » mais certaines applications ont leur propre version de cette bibliothèque. Il est alors nécessaire de mettre à jour ces applications. Les applications concernées sont (se référer à la section documentation) :

- amaya
- dictd
- erlang
- freeamp
- mirrordir
- ppp
- rsync
- vrweb
- gpg
- cvs
- rrdtool
- netscape
- vnc
- kernel
- rpm

## 5 Solution

Installer la version 1.1.4 de la bibliothèque `zlib / libz`. Installer les versions corrigées des logiciels citées ci-dessus (se référer à la section documentation).

## 6 Documentation

- Avis de sécurité RHTSA-2002:027 de Redhat :  
<http://www.redhat.com/support/errata/RHTSA-2002-027.html>
- Avis de sécurité SuSE-SA:2002:010 :  
<http://www.suse.com/us/support/security>
- Site officiel d'amaya  
<http://www.w3c.org/Amaya>
- Site officiel de dictd  
<http://www.dict.org>
- Site officiel de erlang  
<http://www.erlang.org>
- Site officiel de freeamp  
<http://www.freeamp.org>
- Site officiel de mirrordir  
<http://mirrordir.sourceforge.net>
- Site officiel de ppp  
<http://www.samba.org/ppp>
- Site officiel de rsync  
<http://www.rsync.org>
- Site officiel de vrweb  
<http://www.iicm.edu/vrweb>
- Site officiel de gpg  
<http://www.gnupg.org>
- Site officiel de cvs  
<http://www.cvshome.org>

- Site officiel de rrdtool  
<http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/>
- Site officiel de netscape  
<http://www.netscape.com>
- Site officiel de vnc  
<http://www.uk.research.att.com/vnc/>
- Site officiel du kernel  
<http://www.kernel.org>
- Site officiel de rpm  
<http://www.rpm.org>

## **Gestion détaillée du document**

**12 mars 2002** version initiale.