



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 décembre 2004
N° CERTA-2004-AVI-364-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de gzip

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-2004-AVI-364>

Gestion du document

Référence	CERTA-2004-AVI-364-001
Titre	Vulnérabilité de gzip
Date de la première version	09 novembre 2004
Date de la dernière version	10 décembre 2004
Source(s)	Bulletin de sécurité Trustix #2004-0050
Pièce(s) jointe(s)	

TAB. 1 – *Gestion du document*

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

1 Risque

Atteinte à l'intégrité des données.

2 Systèmes affectés

gzip 1.x et versions antérieures.

3 Résumé

Une vulnérabilité découverte dans gzip permet à un utilisateur local, mal intentionné, de porter atteinte à l'intégrité des données présentes sur le système.

4 Description

L'application gzip est un outil de compression, présent dans de nombreuses bibliothèques fournies avec des distributions de Linux et Unix. Les scripts gzexe.in, zdiff.in et znew.in présents dans gzip sont vulnérables à une attaque classique d'écrasement de fichiers via le suivi des liens symboliques. A l'aide de liens habilement constitués, un utilisateur mal intentionné, ayant un accès local au système, peut forcer la modification de fichiers avec les droits de la victime.

5 Solution

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

6 Documentation

- Site Internet de gzip :
<http://www.gzip.org>
- Bulletin de sécurité Trustix #2004-0050 :
<http://www.trustix.org/errata/2004/0050/>
- Bulletin de sécurité Debian DSA-588 du 08 novembre 2004 :
<http://www.debian.org/security/2004/dsa-588>
- Référence CVE CAN-2004-0970 :
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0970>

Gestion détaillée du document

09 novembre 2004 version initiale.

10 décembre 2004 ajout du site Internet de gzip et de la référence au bulletin de sécurité Debian.