

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans 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-2005-AVI-183>

Gestion du document

Référence	CERTA-2005-AVI-183-006
Titre	Vulnérabilités dans <code>gzip</code>
Date de la première version	27 mai 2005
Date de la dernière version	31 août 2005
Source(s)	Bulletin de sécurité FreeBSD du 09 juin 2005
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.

2 Systèmes affectés

`gzip` dans les versions 1.3.5 et versions antérieures.

3 Résumé

Le produit de compression de fichiers `gzip` contient de multiples vulnérabilités permettant à un malveillant d'exécuter du code arbitraire.

4 Description

Ces vulnérabilités permettent l'exécution de commandes arbitraires, modifiant, lors de la décompression, les permissions attribuées à un fichier ou encore installant ces fichiers décompressés, de façon arbitraire dans le système de fichiers.

5 Solution

Tous les utilisateurs de `gzip` doivent mettre à jour leur logiciel de compression.

6 Documentation

- Site Internet de `gzip` :
<http://www.gzip.org/>
- Buletin de sécurité Gentoo GLSA 200505-05 du 09 mai 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200505-05.xml>
- Bulletin de sécurité Mandriva MDKSA-2005:092 du 18 mai 2005 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2005:092>
- Bulletin de sécurité RedHat RHSA-2005:357 du 13 juin 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-357.html>
- Bulletin de sécurité FreeBSD SA-05:11 du 09 juin 2005 :
<ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:11.gzip.asc>
- Bulletin de sécurité Debian DSA-752 du 11 juillet 2005 :
<http://www.debian.org/security/2005/dsa-752>
- Bulletin de sécurité Avaya ASA-2005-172 du 29 août 2005 :
<http://support.avaya.com/elmodocs2/security/ASA-2005-172.pdf>
- Bulletin de sécurité Sun #101816 du 20 juillet 2005 :
<http://sunsolve.sun.com/search/document.do.assetkey=1-26-101816-1>
- Références CVE CAN-2005-0758 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0758>
- Références CVE CAN-2005-0988 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0988>
- Références CVE CAN-2005-1228 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1228>

Gestion détaillée du document

27 mai 2005 version initiale.

03 juin 2005 ajout de la référence au bulletin de sécurité Mandriva.

14 juin 2005 ajout de la référence au bulletin de sécurité RedHat RHSA-2005:357.

15 juin 2005 ajout de la référence au bulletin de sécurité FreeBSD SA-05:11.

12 juillet 2005 ajout de la référence au bulletin de sécurité Debian DSA-752.

21 juillet 2005 ajout de la référence au bulletin de sécurité Sun #101816.

31 août 2005 ajout de la référence au bulletin de sécurité Avaya ASA-2005-172.