

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples 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-2006-AVI-413>

Gestion du document

Référence	CERTA-2006-AVI-413
Titre	Multiples vulnérabilités dans gzip
Date de la première version	28 septembre 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Gentoo GLSA-200609-13 du 23 septembre 2006
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 ;
- déni de service à distance.

2 Systèmes affectés

gzip 1.x.

3 Résumé

De multiples vulnérabilités découvertes dans gzip permettent à un utilisateur distant mal intentionné d'exécuter du code arbitraire ou de provoquer un déni de service.

4 Description

Trois vulnérabilités de type débordement de mémoire ont été découvertes dans les fonctions `make_table()` et `build_tree()`. Ces vulnérabilités peuvent être exploitées au moyen d'une archive compressée au format gzip afin de provoquer un déni de service et/ou d'exécuter du code arbitraire.

Une dernière vulnérabilité de type NULL pointer dans la fonction `huft_build()` permet à une personne malveillante de provoquer un déni de service à distance au moyen d'une archive compressée spécialement contruite.

5 Solution

Se référer aux bulletins de sécurité des éditeurs pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Debian DSA 1181 du 19 septembre 2006 :
<http://www.debian.org/security/2006/dsa-1181>
- Bulletin de sécurité Gentoo GLSA-200609-13 du 23 septembre 2006 :
<http://www.gentoo.org/security/en/glsa/glsa-200609-13.xml>
- Bulletin de sécurité Mandriva MDKSA-2006:167 du 20 septembre 2006 :
<http://wwwnew.mandriva.com/security/advisories?name=MDKSA-2006:167>
- Bulletin de sécurité RedHat RHSA-2006:0667 du 19 septembre 2006 :
<http://rhn.redhat.com/errata/RHSA-2006-0667.html>
- Bulletin de sécurité SuSE SUSE-SA:2006:056 du 26 septembre 2006 :
<http://lists.suse.com/archive/suse-security-announce/2006-Sep/0010.html>
- Bulletin de sécurité Ubuntu USN-349-1 du 19 septembre 2006 :
<http://www.ubuntulinux.org/usn/usn-349-1>
- Bulletin de sécurité FreeBSD FreeBSD-SA-06:24.gzip du 19 septembre 2006 :
<http://security.freebsd.org/advisories/FreeBSD-SA-06:21.gzip.asc>
- Référence CVE CVE-2006-4334 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4334>
- Référence CVE CVE-2006-4335 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4335>
- Référence CVE CVE-2006-4336 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4336>
- Référence CVE CVE-2006-4337 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4337>
- Référence CVE CVE-2006-4338 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4338>

Gestion détaillée du document

28 septembre 2006 version initiale.