

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-2010-AVI-028>

Gestion du document

Référence	CERTA-2010-AVI-028
Titre	Multiples vulnérabilités dans gzip
Date de la première version	22 janvier 2010
Date de la dernière version	–
Source(s)	Avis de sécurité Debian DSA-1974-1 du 20 janvier 2010
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 pour Debian (voir bulletin de l'éditeur) ;
- gzip pour Red Hat (voir bulletin de l'éditeur) ;
- gzip pour Ubuntu (voir bulletin de l'éditeur) ;
- gzip pour Mandriva (voir bulletin de l'éditeur) ;
- GNU gzip (voir bulletin de l'éditeur).

3 Résumé

Deux vulnérabilités dans gzip permettent l'exécution de code arbitraire à distance.

4 Description

- Une vulnérabilité dans la décompression des blocs de données *Huffman* permet l'exécution de code arbitraire à distance ;
- une vulnérabilité liée à un débordement d'entier lors de la décompression de données compressées via l'algorithme *Lempel-Ziv-Welch (LZW)* permet l'exécution de code arbitraire à distance.

5 Solution

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

6 Documentation

- Bulletin de sécurité Debian DSA-1974-1 du 20 janvier 2010 :
<http://www.debian.org/security/2010/dsa-1974>
- Bulletin de sécurité Mandriva MDVSA-2010:019 du 20 janvier 2010 :
<http://www.mandriva.com/archives/security/advisories?name=MDVSA-2010:019>
- Bulletin de sécurité Mandriva MDVSA-2010:020 du 20 janvier 2010 :
<http://www.mandriva.com/archives/security/advisories?name=MDVSA-2010:020>
- Bulletin de sécurité RedHat RHSA-2010:0061 du 20 janvier 2010 :
<http://rhn.redhat.com/errata/RHSA-2010-0061.html>
- Bulletin de sécurité Ubuntu USN-889-1 du 20 janvier 2010 :
<http://www.ubuntulinux.org/usn/usn-889-1>
- Information de sécurité GNU :
http://savannah.gnu.org/forum/forum.php?forum_id=615
- Référence CVE CVE-2009-2624 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2624>
- Référence CVE CVE-2010-0001 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0001>

Gestion détaillée du document

22 janvier 2010 version initiale.