



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 avril 2008
N° CERTA-2008-AVI-186

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans UnZip

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-2008-AVI-186>

Gestion du document

Référence	CERTA-2008-AVI-186
Titre	Vulnérabilité dans UnZip
Date de la première version	08 avril 2008
Date de la dernière version	–
Source(s)	Mise à jour Red Hat RHSA-2008:0196-3 du 18 mars 2008
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

- Les versions de UnZip antérieures à 5.52-9etch1 pour les distributions Debian stables (etch) ;
- les versions de UnZip antérieures à 5.50-31.EL2 et 5.50-36.EL3 pour les distributions Red Hat ;
- les versions de UnZip antérieures à 5.50-9.4 et 5.52-3.1 pour les distributions Mandriva.

3 Résumé

Une vulnérabilité a été identifiée dans l'utilitaire UnZip. L'exploitation de celle-ci peut conduire à exécuter du code arbitraire sur un système vulnérable sous certaines conditions.

4 Description

Une vulnérabilité a été identifiée dans l'utilitaire UnZip. Elle concerne la macro NEEDBITS de la fonction `inflate_dynamic()` dans le fichier `inflate.c`.

L'exploitation de cette vulnérabilité à l'ouverture d'un fichier spécialement construit peut perturber le système, voire exécuter des commandes arbitraires sur celui-ci.

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 1522 du 17 mars 2008 :
<http://www.debian.org/security/2008/dsa-1522>
- Bulletin de sécurité Ubuntu USN-589-1 du 20 mars 2008 :
<http://www.ubuntulinux.org/usn/usn-589-1>
- Bulletin de sécurité Red Hat RHSA-2008:0196-3 du 18 mars 2008 :
<http://rhn.redhat.com/errata/RHSA-2008-0196.html>
- Bulletin de sécurité Gentoo GLSA 200804-06 du 06 avril 2008 :
<http://www.gentoo.org/security/en/glsa/glsa-200804-06.xml>
- Bulletin de sécurité Mandriva MDVSA-2008:068 du 18 mars 2008 :
<http://www.mandriva.com/en/security/advisories?name=MDVSA-2008:068>
- Bulletin de sécurité rPath 2008-0116-1 du 21 mars 2008 :
<http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0116>
- Référence CVE CVE-2008-0888 :
<http://cve.mitre.org/cgi-bin/cvname.cgi?name=CVE-2008-0888>

Gestion détaillée du document

08 avril 2008 version initiale.