

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans la bibliothèque libpng

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-212>

Gestion du document

Référence	CERTA-2004-AVI-212-002
Titre	Vulnérabilité dans la bibliothèque libpng
Date de la première version	30 juin 2004
Date de la dernière version	09 juillet 2004
Source(s)	Avis de sécurité Debian DSA-213 du 19 décembre 2002
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

- Déni de service ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

Tout système ayant une bibliothèque libpng.

3 Résumé

Plusieurs vulnérabilités présentes dans la bibliothèque libpng permettent à un utilisateur mal intentionné d'exécuter du code arbitraire ou d'entraîner un déni de service sur la machine cible.

4 Description

La bibliothèque libpng est utilisée par de nombreuses applications (dont les navigateurs) pour la manipulation de fichiers image au format png (Portable Neutral Graphics).

Plusieurs vulnérabilités dans la bibliothèque `libpng`, en plus de celles corrigées par le premier correctif, permettent à un utilisateur mal intentionné d'exécuter du code arbitraire ou d'entraîner un déni de service sur la machine cible au moyen d'un fichier judicieusement composé.

Le premier avis du CERTA relatif à la vulnérabilité de `libpng` est l'avis CERTA-2003-AVI-003 du 14 janvier 2003 :

<http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-003/>

5 Solution

Se référer aux bulletins de sécurité des différents éditeurs pour connaître la disponibilité des correctifs (cf. section Documentation).

6 Documentation

- Site Internet de la bibliothèque `libpng` :
<http://www.libpng.org/pub/png/libpng.html>
- Bulletin de sécurité RedHat RHSA-2004:249 du 18 juin 2004 :
<http://rhn.redhat.com/errata/RHSA-2004-249.html>
- Bulletin de sécurité Mandrake MDKSA-2004:063 du 29 juin 2004 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:063>
- Bulletin de sécurité Gentoo GLSA 200407-06 du 08 juillet 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200407-06.xml>
- Bulletin de sécurité OpenBSD pour `png` du 07 juillet 2004 :
<http://www.vuxml.org/openbsd/>
- Référence CVE CAN-2002-1363 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1363>

Gestion détaillée du document

30 juin 2004 version initiale.

07 juillet 2004 ajout de la référence au bulletin de sécurité OpenBSD.

09 juillet 2004 ajout de la référence au bulletin de sécurité Gentoo.