

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de la bibliothèque gd

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-360>

Gestion du document

Référence	CERTA-2004-AVI-360-005
Titre	Vulnérabilité de la bibliothèque gd
Date de la première version	04 novembre 2004
Date de la dernière version	20 décembre 2004
Source(s)	Bulletin de sécurité GLSA 200411-08 de Gentoo
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

gd versions 2.0.28 et antérieures.

3 Description

gd est une bibliothèque graphique utilisée pour la manipulation d'images de différents formats (GIF, JPEG, PNG, ...).

Une vulnérabilité de type débordement de mémoire est présente dans une routine réalisant le chargement des images au format PNG.

Au moyen d'une image au format PNG habilement constituée, cette vulnérabilité peut être exploitée par un utilisateur mal intentionné afin d'exécuter du code arbitraire via une application utilisant la bibliothèque vulnérable.

4 Solution

La version 2.0.29 de la bibliothèque `gd` corrige cette vulnérabilité.

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

5 Documentation

- Site Internet de `gd` :
<http://www.boutell.com/gd>
- Bulletin de sécurité Gentoo GLSA 200411-08 du 03 novembre 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200411-08.xml>
- Bulletin de sécurité Debian DSA-589 du 09 novembre 2004 :
<http://www.debian.org/security/2004/dsa-589>
- Bulletin de sécurité Debian DSA-591 du 09 novembre 2004 :
<http://www.debian.org/security/2004/dsa-591>
- Bulletin de sécurité Mandrake MDKSA-2004:132 du 15 novembre 2004 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:132>
- Bulletin de sécurité Debian DSA-601 du 29 novembre 2004 :
<http://www.debian.org/security/2004/dsa-601>
- Bulletin de sécurité Debian DSA-602 du 29 novembre 2004 :
<http://www.debian.org/security/2004/dsa-602>
- Bulletin de sécurité Red Hat RHSA-2004:638 du 17 décembre 2004 :
<http://rhn.redhat.com/errata/RHSA-2004-638.html>
- Bulletin de sécurité FreeBSD pour `gd` du 05 novembre 2004 :
<http://www.vuxml.org/freebsd>
- Référence CVE CAN-2004-0990 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0990>

Gestion détaillée du document

04 novembre 2004 version initiale.

16 novembre 2004 ajout des références aux bulletins de sécurité de Debian.

19 novembre 2004 ajout de la référence au bulletin de sécurité de Mandrake.

29 novembre 2004 ajout de la référence au bulletin de sécurité de Debian DSA-601.

30 novembre 2004 ajout de la référence au bulletin de sécurité de Debian DSA-602.

20 décembre 2004 ajout de la référence aux bulletins de sécurité de Red Hat et FreeBSD.