Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 novembre 2005
N° CERTA-2005-AVI-440-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans la bibliothèque libungif/giflib

Gestion du document

Référence	CERTA-2005-AVI-440-003
Titre	Multiples vulnérabilités dans la bibliothèque libungif/giflib
Date de la première version	07 novembre 2005
Date de la dernière version	10 novembre 2005
Source(s)	Bulletin de sécurité RedHat Bugzilla #171413
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

- libungif 4.1.3 et versions antérieures ;
- giflib 4.1.3 et versions antérieures.

3 Résumé

Deux vulnérabilités affectant les bibliothèques `libungif` et `giflib` permettent à un utilisateur distant mal intentionné de provoquer un déni de service ou d'exécuter du code arbitraire.

4 Description

Les bibliothèques `libungif` et `giflib` permettent le traitement des fichiers images au format `gif`.

– Une vulnérabilité dans la gestion des pointeurs peut être exploitée via un fichier image au format `gif` afin de provoquer à distance l'arrêt brutal de l'application ;
– une vulnérabilité de type débordement de mémoire permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance au moyen d'un fichier image au format `gif` malicieusement construit.

5 Solution

Mettre à jour la bibliothèque `libungif` en passant à la version 4.1.4 disponible à l'adresse suivante :
http://sourceforge.net/project/showfiles.php?group_id=102202&package_id=109698

Mettre à jour la bibliothèque `giflib` en passant à la version 4.1.4 disponible à l'adresse suivante :
http://sourceforge.net/project/showfiles.php?group_id=102202&package_id=119585

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

6 Documentation

– Bulletin de sécurité RedHat Bugzilla #17141 :
https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=171413
– Bulletin de sécurité RedHat RHSA-2005-828 du 03 novembre 2005 :
http://rhn.redhat.com/errata/RHSA-2005-828.html
– Bulletin de sécurité Gentoo GLSA 200511-03 du 04 novembre 2005 :
http://www.gentoo.org/security/en/glsa/glsa-200511-03.xml
– Bulletin de sécurité Debian DSA-890 du 09 novembre 2005 :
http://www.debian.org/security/2005/dsa-890
– Bulletin de sécurité Mandriva MDKSA-2005:207 du 09 novembre 2005 :
http://www.mandriva.com/security/advisories?name=MDKSA-2005:207
– Bulletin de sécurité Ubuntu USN-214 du 07 novembre 2005 :
http://lists.ubuntu.com/archives/ubuntu-security-announce/2005-November/000240.html
– Mise à jour de `libungif` pour Fedora Core 3 :
http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/
– Mise à jour de `libungif` pour Fedora Core 4 :
http://download.fedora.redhat.com/pub/fedora/linux/core/updates/4/
– Référence CVE CAN-2005-2974 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2974
– Référence CVE CAN-2005-3350 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3350

Gestion détaillée du document

07 novembre 2005 version initiale.
08 novembre 2005 ajout de la référence au bulletin de sécurité Ubuntu USN-214.
09 novembre 2005 ajout de la référence au bulletin de sécurité Debian DSA-890.
10 novembre 2003 ajout de la référence au bulletin de sécurité Mandriva MDKSA-2005:207.