



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 octobre 2007
N° CERTA-2006-AVI-329-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans la bibliothèque libTIFF

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-2006-AVI-329>

Gestion du document

Référence	CERTA-2006-AVI-329-002
Titre	Multiples vulnérabilités dans la bibliothèque libTIFF
Date de la première version	04 août 2006
Date de la dernière version	17 octobre 2007
Source(s)	Bulletin de sécurité Ubuntu USN-330-1 du 02 août 2006
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 ;
- déni de service à distance.

2 Systèmes affectés

libTIFF 3.x.

Toutes les applications faisant appel à la bibliothèque vulnérable sont affectées par ces vulnérabilités.

3 Description

Plusieurs vulnérabilités de type débordement de mémoire ont été découvertes dans la bibliothèque libTIFF. Ces vulnérabilités permettent à un utilisateur distant mal intentionné de provoquer un déni de service ou d'exécuter du code arbitraire. Un individu malveillant peut exploiter ces vulnérabilités au moyen d'une image au format TIFF (*Tag Image File Format*) spécialement conçue.

4 Solution

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

5 Documentation

- Bulletin de sécurité Debian DSA 1137 du 02 août 2006 :
<http://www.debian.org/security/2006/dsa-1137>
- Bulletin de sécurité RedHat RHSA-2006:0603 du 02 août 2006 :
<http://rhn.redhat.com/errata/RHSA-2006-0603.html>
- Bulletin de sécurité SUSE SuSE-SA:2006:044 du 01 août 2006 :
<http://lists.suse.com/archive/suse-security-announce/2006-Aug/0001.html>
- Bulletin de sécurité Ubuntu USN-330-1 du 02 août 2006 :
<http://www.ubuntu.org/usn/usn-330-1>
- Bulletin de sécurité Gentoo GLSA 200608-07 du 04 août 2006 :
<http://www.gentoo.org/security/en/glsa/glsa-200608-07.xml>
- Bulletin de sécurité Mandriva MDKSA-2006:137 du 01 août 2006 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2006:137>
- Bulletin de sécurité Avaya ASA-2006-166 du 16 août 2006 :
<http://support.avaya.com/elmodocs2/security/ASA-2006-166.htm>
- Bulletin de sécurité Sun 103099 du 11 octobre 2007 :
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-103099-1>
- Référence CVE CVE-2006-3459 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3459>
- Référence CVE CVE-2006-3460 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3460>
- Référence CVE CVE-2006-3461 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3461>
- Référence CVE CVE-2006-3462 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3462>
- Référence CVE CVE-2006-3463 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3463>
- Référence CVE CVE-2006-3464 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3464>
- Référence CVE CVE-2006-3465 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3465>

Gestion détaillée du document

04 août 2006 version initiale.

18 août 2006 ajout des références aux bulletins de sécurité Gentoo, Mandriva et Avaya.

17 octobre 2007 ajout de la référence au bulletin de sécurité Sun.