



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 février 2005
N° CERTA-2004-AVI-418-005

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Xpdf et applications associées

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-418>

Gestion du document

Référence	CERTA-2004-AVI-418-005
Titre	Vulnérabilité de Xpdf
Date de la première version	30 décembre 2004
Date de la dernière version	17 février 2005
Source(s)	Bulletin de sécurité iDefense du 21 décembre 2004
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.

2 Systèmes affectés

Lecteur *Xpdf* de documents au format Portable Document Format (PDF).

D'autres applications utilisant une partie du code de *Xpdf* sont également vulnérables (Gpdf, kdegraphics, koffice, tetex, ...).

3 Résumé

Une vulnérabilité du lecteur *Xpdf* permet à un utilisateur mal intentionné d'exécuter du code arbitraire sur une machine vulnérable.

4 Description

Une vulnérabilité de type débordement de mémoire a été découverte dans la fonction *Gfx::doImage*.

Un utilisateur mal intentionné peut exploiter cette vulnérabilité par le biais d'un document au format PDF habilement construit. Il est alors possible d'exécuter du code arbitraire avec les privilèges de l'utilisateur ayant lancé le lecteur *Xpdf*.

5 Contournement provisoire

Ne lire que des documents au format PDF provenant d'une source de confiance.

6 Solution

Mettre à jour le lecteur *Xpdf* (cf. section Documentation).

7 Documentation

- Site Internet du lecteur *Xpdf* :
<http://www.foolabs.com/xpdf/>
- Correctif pour le lecteur *Xpdf* :
<ftp://ftp.foolabs.com/pub/xpdf/xpdf-3.00pl2.patch>
- Bulletin de sécurité de iDefense du 21 décembre 2004 :
<http://www.iddefense.com/application/poi/display?id=172>
- Bulletin de sécurité Debian DSA-619 du 30 décembre 2004 :
<http://www.debian.org/security/2004/dsa-619>
- Bulletin de sécurité Gentoo GLSA-200412-24 du 28 décembre 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200412-24.xml>
- Bulletin de sécurité Gentoo GLSA-200501-17 du 11 janvier 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200501-17.xml>
- Bulletin de sécurité Mandrake MDKSA-2004-161 pour *Xpdf* du 29 décembre 2004 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:161>
- Bulletin de sécurité Mandrake MDKSA-2004-162 pour *Gpdf* du 29 décembre 2004 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:162>
- Bulletin de sécurité Mandrake MDKSA-2004-163 pour *kdegraphics* du 29 décembre 2004 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:163>
- Bulletin de sécurité Mandrake MDKSA-2004-165 pour *koffice* du 29 décembre 2004 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:165>
- Bulletin de sécurité Mandrake MDKSA-2004-166 pour *tetex* du 29 décembre 2004 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:166>
- Bulletin de sécurité RedHat RHSA-2005:018 du 12 janvier 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-018.html>
- Bulletin de sécurité RedHat RHSA-2005:034 du 15 janvier 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-034.html>
- Bulletin de sécurité RedHat RHSA-2005:066 du 15 janvier 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-066.html>
- Bulletin de sécurité FreeBSD pour *Xpdf* du 23 décembre 2004 :
<http://www.vuxml.org/freebsd/>
- Bulletin de sécurité OpenBSD pour *Xpdf* du 22 décembre 2004 :
<http://www.vuxml.org/openbsd>
- Bulletin de sécurité OpenBSD pour *tetex* du 25 décembre 2004 :
<http://www.vuxml.org/openbsd>
- Référence CVE CAN-2004-1125 :
<http://cve.mitre.org/cgi-bin/cvname.cgi?name=CAN-2004-1125>

Gestion détaillée du document

30 décembre 2004 version initiale.

03 janvier 2005 première révision : ajout des applications associées et ajout des avis Debian et Mandrake.

12 janvier 2005 ajout référence au bulletin de sécurité Gentoo GLSA 200501-17.

14 janvier 2005 ajout référence au bulletin de sécurité RedHat RHSA-2005:018.

20 janvier 2005 modification du lien vers le serveur de Foolabs.

17 février 2005 ajout des références aux bulletins de sécurité RedHat.