

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Adobe Acrobat Reader sous Unix

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-398>

Gestion du document

Référence	CERTA-2004-AVI-398-004
Titre	Vulnérabilité de Adobe Acrobat Reader sous Unix
Date de la première version	15 décembre 2004
Date de la dernière version	03 janvier 2005
Source(s)	Bulletin de sécurité iDEFENSE "Adobe Acrobat Reader 5.0.9 for Unix" du 14 décembre 2004
Pièce(s) jointe(s)	

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

Adobe Acrobat Reader for Unix version 5.0.9 et antérieures.

3 Résumé

Une vulnérabilité découverte dans l'application Acrobat Reader d'Adobe permet à un utilisateur mal intentionné d'exécuter du code arbitraire sur le système vulnérable.

4 Description

L'application Adobe Acrobat Reader for Unix permet de lire et de manipuler les fichiers de type PDF (Portable Document Format) sur les systèmes d'exploitation descendant d'Unix.

La fonction `mailListIsPdf()` permet de vérifier si le fichier fourni en entrée est un message électronique contenant une pièce jointe de type PDF. Cette fonction présente une vulnérabilité de type dépassement de mémoire qui permet à un utilisateur mal intentionné d'exécuter du code arbitraire sur le système vulnérable avec les privilèges de la victime. Une personne malveillante peut exécuter du code arbitraire à distance, au moyen d'un message électronique ayant comme pièce jointe un fichier pdf malicieusement constitué.

5 Solution

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

6 Documentation

- Site Internet Adobe :
<http://www.adobe.com/products/acrobat/readermain.html>
- Bulletin de sécurité iDEFENSE “Adobe Acrobat Reader 5.0.9 mailListIsPdf() Buffer Overflow Vulnerability” du 14 décembre 2004 :
<http://www.odefense.com/application/poi/display?id=161&type=vulnerabilities>
- Bulletin de sécurité d'Adobe :
<http://www.adobe.com/support/techdocs/331153.html>
- Bulletin de sécurité Gentoo GLSA-200412-12 du 16 décembre 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200412-12.xml>
- Bulletin de sécurité Red hat RHSA-2004:674 du 23 décembre 2004 :
<http://rhn.redhat.com/errata/RHSA-2004-674.html>
- Bulletin de sécurité FreeBSD du 21 décembre 2004 :
<http://www.vuxml.org/freebsd/>
- Bulletin de sécurité OpenBSD du 22 décembre 2004 :
<http://www.vuxml.org/openbsd/>
- Référence CVE CAN-2004-1152 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1152>

Gestion détaillée du document

15 décembre 2004 version initiale.

20 décembre 2004 ajout référence au bulletin de sécurité de Gentoo.

22 décembre 2004 ajout référence au bulletin de sécurité de FreeBSD.

23 décembre 2004 ajout référence au bulletin de sécurité d'OpenBSD.

03 janvier 2005 ajout référence au bulletin de sécurité de Red Hat.