

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Adobe Acrobat Reader

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-397>

Gestion du document

Référence	CERTA-2004-AVI-397
Titre	Vulnérabilité de Adobe Acrobat Reader
Date de la première version	15 décembre 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité iDEFENSE “Adobe Acrobat Reader 6.0” 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 à distance.

2 Systèmes affectés

- Adobe Acrobat Reader 6.0.2 et versions antérieures ;
- Adobe Acrobat Professionnal & Standard 6.0.2 et versions antérieures.

Les systèmes affectés touchent les systèmes d'exploitation Microsoft Windows et Mac d'Apple.

3 Résumé

Une vulnérabilité présente dans les applications Adobe Acrobat Reader et Adobe Acrobat Professionnal & Standard permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance avec les privilèges de la victime.

4 Description

Les applications Adobe Acrobat Reader et Adobe Acrobat Professionnal & Standard permettent principalement de manipuler les fichiers de type PDF (Portable Document Format).

Une vulnérabilité de type chaîne de format est présente dans la gestion des fichiers .etd. Elle permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance avec les privilèges de la victime, à l'aide d'un message électronique ayant comme pièce jointe un fichier PDF malicieusement constitué. Ce fichier PDF malicieusement constitué peut également être appelé au moyen d'une adresse réticulaire URL contenue dans le corps du message électronique.

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 6.0 .ETD File Format String Vulnerability" du 14 décembre 2004 :
<http://www.odefense.com/application/poi/display?id=163&type=vulnerabilities>
- Mise à jour Adobe Acrobat Reader 6.0.3 pour Windows :
<http://www.adobe.com/support/downloads/detail.jsp?ftpID=2679>
- Mise à jour Adobe Acrobat Reader 6.0.3 pour Mac :
<http://www.adobe.com/support/downloads/detail.jsp?ftpID=2680>
- Mise à jour Adobe Acrobat Professionnal & Standard 6.0.3 pour Windows :
<http://www.adobe.com/support/downloads/detail.jsp?ftpID=2677>
- Mise à jour Adobe Acrobat Professionnal & Standard 6.0.3 pour Mac :
<http://www.adobe.com/support/downloads/detail.jsp?ftpID=2676>
- Référence CVE CAN-2004-1153 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1153>

Gestion détaillée du document

15 décembre 2004 version initiale.