



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 06 octobre 2010
N° CERTA-2010-AVI-470

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Adobe Reader et Adobe Acrobat

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-2010-AVI-470>

Gestion du document

Référence	CERTA-2010-AVI-470
Titre	Vulnérabilité dans Adobe Reader et Adobe Acrobat
Date de la première version	06 octobre 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Adobe APSB10-21 du 05 octobre 2010
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.

2 Systèmes affectés

- Adobe Reader et Adobe Acrobat version 9.3.4 et antérieures, pour toutes plateformes ;
- Adobe Reader et Adobe Acrobat version 8.2.4 et antérieures, pour toutes plateformes.

3 Résumé

Une vulnérabilité permettant de l'exécution de code arbitraire à distance affecte Adobe Reader et Adobe Acrobat.

4 Description

Une vulnérabilité dans le module de traitement des polices de caractère d'Adobe Reader et Adobe Acrobat (*CoolType.dll*) permet l'exécution de code arbitraire à distance.

Cette vulnérabilité est actuellement activement exploitée sur l'Internet. Le code d'exploitation semble fonctionner sur de nombreuses plateformes, incluant Microsoft Windows 7 et Microsoft Vista et a la capacité de contourner les mécanismes de protection de type ASLR (*Address Space Layout Randomization*) et DEP (*Data Execution Prevention*).

5 Solution

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

6 Documentation

- Bulletin de sécurité Adobe apsb10-21 du 05 octobre 2010 :
<http://www.adobe.com/support/security/bulletins/apsb10-21.html>
- Référence CVE CVE-2010-2883 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2883>
- Référence CVE CVE-2010-2884 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2884>
- Référence CVE CVE-2010-2887 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2887>
- Référence CVE CVE-2010-2888 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2888>
- Référence CVE CVE-2010-2889 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2889>
- Référence CVE CVE-2010-2890 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2890>
- Référence CVE CVE-2010-3619 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3619>
- Référence CVE CVE-2010-3620 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3620>
- Référence CVE CVE-2010-3621 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3621>
- Référence CVE CVE-2010-3622 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3622>
- Référence CVE CVE-2010-3623 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3623>
- Référence CVE CVE-2010-3624 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3624>
- Référence CVE CVE-2010-3625 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3625>
- Référence CVE CVE-2010-3626 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3626>
- Référence CVE CVE-2010-3627 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3627>
- Référence CVE CVE-2010-3628 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3628>
- Référence CVE CVE-2010-3629 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3629>
- Référence CVE CVE-2010-3630 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3630>
- Référence CVE CVE-2010-3631 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3631>
- Référence CVE CVE-2010-3632 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3632>

- Référence CVE CVE-2010-3656 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3656>
- Référence CVE CVE-2010-3657 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3657>
- Référence CVE CVE-2010-3658 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3658>

Gestion détaillée du document

06 octobre 2010 version initiale.