

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans Adobe Reader et 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-2011-ALE-008>

Gestion du document

Référence	CERTA-2011-ALE-008-002
Titre	Vulnérabilité dans Adobe Reader et Acrobat
Date de la première version	07 décembre 2011
Date de la dernière version	10 janvier 2012
Source	Alerte de sécurité Adobe APSA11-04 du 16 décembre 2011
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 X (10.1.1) et versions 10.x antérieures pour systèmes Windows et Macintosh ;
- Adobe Reader 9.4.6 et versions 9.x antérieures pour systèmes Windows, Macintosh et UNIX ;
- Adobe Acrobat X (10.1.1) et versions 10.x antérieures pour systèmes Windows et Macintosh ;
- Adobe Acrobat 9.4.6 et versions 9.x antérieures pour systèmes Windows et Macintosh.

3 Résumé

Une vulnérabilité permettant l'exécution de code arbitraire à distance affecte les produits Adobe Acrobat et Adobe Reader. Celle-ci est actuellement exploitée.

Un correctif est publié pour la version 9 des deux produits.

4 Description

Les logiciels Adobe Acrobat et Adobe Reader sont vulnérables à une faille permettant à une personne mal-intentionnée d'exécuter du code arbitraire à distance. Elle est actuellement exploitée sur l'Internet au moyen de document PDF spécialement conçus.

5 Contournement provisoire

Il est possible, dans les versions 10.n (ou X.n) de ces produits, d'activer des modes de protection (*Protected Mode* pour Adobe Reader et *Protected View* pour Adobe Acrobat) pour rendre plus difficile l'exploitation de cette vulnérabilité. Adobe annonce qu'un correctif pour ces versions sera publié le 10 janvier 2012.

Le CERTA recommande l'utilisation d'un logiciel alternatif tant qu'un correctif n'est pas disponible.

Mise à jour du 19 décembre 2011 : la version 9.4.7 de chacun des deux produits corrige le problème. Mise à jour du 10 janvier 2012 : les versions 9.5 et 10.1.2 de chacun des deux produits corrigent le problème.

6 Solution

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

7 Documentation

- Alerte de sécurité Adobe APSA11-04 du 16 décembre 2011 :
<http://www.adobe.com/support/security/advisories/apsa11-04.html>
- Bulletin de sécurité Adobe APSB11-30 du 16 décembre 2011 :
<http://www.adobe.com/support/security/bulletins/apsb11-30.html>
- Bulletin de sécurité Adobe APSB12-01 du 10 janvier 2012 :
<http://www.adobe.com/support/security/bulletins/apsb12-01.html>
- Avis du CERTA CERTA-2011-AVI-705 du 19 décembre 2011 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-705/index.html>
- Avis du CERTA CERTA-2012-AVI-014 du 10 janvier 2012 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-014/index.html>
- Référence CVE CVE-2011-2462 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2462>

Gestion détaillée du document

07 décembre 2011 version initiale.

19 décembre 2011 publication d'un correctif pour les versions 9.

10 janvier 2012 publication d'un correctif pour les versions 10.