



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 02 septembre 2004
N° CERTA-2004-AVI-270-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités d'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-2004-AVI-270>

Gestion du document

Référence	CERTA-2004-AVI-270-003
Titre	Vulnérabilités d'Adobe Acrobat
Date de la première version	17 août 2004
Date de la dernière version	02 septembre 2004
Source(s)	Bulletin de sécurité iDefense du 12 août 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 à distance ;
- déni de service.

2 Systèmes affectés

- Vulnérabilité CVE CAN-2004-0629 : Adobe Acrobat et Adobe Acrobat Reader versions antérieures à la 6.0.2 ;
- vulnérabilité CVE CAN-2004-0630 et CVE CAN 2004-0631 : Adobe Acrobat Reader versions 5.0.8 et antérieures pour les plates-formes Unix.

3 Résumé

Plusieurs vulnérabilités des applications Adobe Acrobat et Adobe Acrobat Reader permettent à un utilisateur distant mal intentionné d'exécuter du code arbitraire ou de provoquer un déni de service sur une machine vulnérable.

4 Description

- Vulnérabilité CVE CAN-2004-0629 : une vulnérabilité de type débordement de mémoire a été découverte dans le composant ActiveX. Elle permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire ou de provoquer un déni de service.
- Vulnérabilité CVE CAN-2004-0630 et CAN-2004-0631 : deux vulnérabilités dans le décodage des chaînes "uuencodées" sur les plates-formes Unix permettent à un utilisateur d'exécuter du code arbitraire par le biais d'un document au format PDF malicieusement construit.

5 Contournement provisoire

- Vulnérabilité CVE CAN-2004-0629 : ne pas ouvrir les documents au format PDF avec un navigateur.
- Vulnérabilité CVE CAN-2004-0630 et CAN-2004-0631 :
 - n'ouvrir que les documents PDF provenant d'une source de confiance ;
 - ne pas ouvrir les documents PDF sur une plate-forme Unix.

6 Solution

- La version 5.0.9 corrige les vulnérabilités CVE CAN-2004-0630 et CAN-2004-0631 ;
- la version 6.0.2 corrige la vulnérabilité CVE CAN-2004-0629.

Adobe Acrobat Reader est téléchargeable à l'adresse suivante :
<http://www.adobe.com/products/acrobat/alternate.html>

7 Documentation

- Site Internet du produit Adobe Acrobat :
<http://www.adobe.com/products/acrobat/main.html>
- Bulletin de sécurité iDefense du 12 août 2004 (CVE CAN-2004-0630) :
<http://www.iddefense.com/application/poi/display?id=124>
- Bulletin de sécurité iDefense du 12 août 2004 (CVE CAN-2004-0631) :
<http://www.iddefense.com/application/poi/display?id=125>
- Bulletin de sécurité iDefense du 13 août 2004 (CVE CAN-2004-0629) :
<http://www.iddefense.com/application/poi/display?id=126>
- Bulletin de sécurité Gentoo GLSA-200408-14 du 15 août 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200408-14.xml>
- Bulletin de sécurité RedHat RHSA-2004:432 du 26 août 2004 :
<http://rhn.redhat.com/errata/RHSA-2004-432.html>
- Bulletin de sécurité FreeBSD pour acroread du 12 août 2004 :
<http://www.vuxml.org/freebsd/>
- Mise à jour de sécurité du paquetage NetBSD acroread5 :
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/print/acroread5/README.html>
- Référence CVE CAN-2004-0629 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0629>
- Référence CVE CAN-2004-0630 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0630>
- Référence CVE CAN-2004-0631 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0631>

Gestion détaillée du document

17 août 2004 version initiale.

27 août 2004 ajout de la référence au bulletin de sécurité RedHat.

30 août 2004 ajout de la référence au bulletin de sécurité NetBSD et des liens vers les références CVE.
02 septembre 2004 ajout du lien Internet de téléchargement de Adobe Acrobat Reader.