

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans l'implémentation des logiciels de lecture des documents PDF

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-2003-ALE-001>

Gestion du document

Référence	CERTA-2003-ALE-001-001
Titre	Vulnérabilité dans l'implémentation des logiciels de lecture des documents PDF
Date de la première version	23 juin 2003
Date de la dernière version	4 juillet 2003
Source(s)	CVE CAN-2003-0434 Avis RedHat RHSA-2003:196
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 commandes arbitraires.

2 Systèmes affectés

- xpdf dans ses versions antérieures à 2.02p1 sur Unix ;
- Acrobat Reader dans ses version antérieures à 5.07 sur Unix ;
- une liste des distributions vulnérables est disponible sur le site du CERT/CC.

3 Résumé

Le format PDF est généralement présenté comme un format de document inoffensif, ce qui le rend particulièrement dangereux lorsqu'une vulnérabilité est découverte.

Une personne mal intentionnée peut fabriquer un document PDF contenant une URL astucieusement constituée qui, lorsque le lecteur choisit de la suivre, permet d'exécuter un code arbitraire en « *script shell* ».

4 Description

Le format PDF permet dans une certaine mesure l'interactivité avec le lecteur du document. En particulier, le format permet de définir des liens (URI) dans un document. La mise en œuvre de la gestion de cette interactivité dans les logiciels de lecture des fichiers PDF peut laisser, sous certaines conditions, la possibilité d'exécuter du code malveillant avec les privilèges de la victime.

Les versions du logiciel `xpdf` antérieures à 2.02pl1 sont vulnérables et permettent dans certaines configurations, l'exécution de « *scripts shell* ».

Les versions du logiciel `Acrobat Reader` antérieures à 5.06 sur Unix sont aussi vulnérables.

Remarque : la vulnérabilité exploite des possibilités du langage de commandes d'Unix (le *shell*). Elle n'est donc pas spécifique à une architecture particulière (microprocesseur, bibliothèque partagée, noyau, ...). Le fait que le code exécuté soit du script plutôt que du code assembleur rend cette vulnérabilité *a priori* très portable.

5 Contournement provisoire

On peut détecter un document PDF exploitant cette vulnérabilité avec la commande :

```
$ grep -a /URI document.pdf | perl -pe 's|.*URI \(([^\ ]+)\)|$1|'
```

Le résultat doit être une adresse électronique et ne doit pas contenir de commande du *shell*.

6 Solution

Des correctifs sont disponibles pour `Acrobat Reader` et `xpdf`.

7 Documentation

- `xpdf` :
<http://www.foolabs.com/xpdf>
- `Acrobat Reader` pour Unix :
<ftp://ftp.adobe.com/pub/adobe/acrobatreader/unix/5.x>
- liste des distributions vulnérables :
<http://www.kb.cert.org/vuls/id/200132>
- Récapitulatif sur la vulnérabilité dans la base CVE :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0434>
- Certaines distributions Red Hat permettent l'exploitation de cette vulnérabilité, le correctif est disponible :
<http://rhn.redhat.com/errata/RHSA-2003-196.html>
- Mandrake a publié un correctif pour cette vulnérabilité :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:071>

Gestion détaillée du document

23 juin 2003 version initiale ;

04 juillet 2003 correctifs Mandrake.