Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 04 août 2006
N° CERTA-2006-AVI-271-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités sur OpenOffice

Gestion du document

Référence	CERTA-2006-AVI-271-002
Titre	Multiples vulnérabilités sur OpenOffice
Date de la première version	30 juin 2006
Date de la dernière version	04 août 2006
Source(s)	Bulletin de sécurité OpenOffice
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 ;
- déni de service.

2 Systèmes affectés

- OpenOffice 1.1.x ;
- OpenOffice.org 2.x.

3 Résumé

Plusieurs vulnérabilités sont présentes dans OpenOffice. Ces vulnérabilités peuvent être utilisées par un utilisateurs mal intentionné pour exécuter du code arbitraire sur le système ou réaliser un déni de service.

4 Description

- Une vulnérabilité est présente dans le traitement de certaines applet java dans les documents OpenOffice. Cette vulnérabilité peut être exploitée pour coutourner le « bac à sable » de la machine java et obtenir les privilèges de l'utilisateur sur le système.

- Une seconde vulnérabilité existe dans le traitement des macros embarquées dans les documents OpenOffice. Cette vulnérabilité peut être utilisée pour faire exécuter du code malveillant à l'ouverture d'une document habilement construit.
- Une troisième vulnérabilité existe dans le traitement des documents XML. Cette vulnérabilité de type débordement de mémoire peut être exploitée pour exécuter du code arbitraire sur le système.

5 Solution

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

6 Documentation

- Bulletin de sécurité OpenOffice :
  http://www.openoffice.org/security/bulletin-20060629.html
- Bulletin de sécurité Red Hat RHSA-2006-0573 du 03 juillet 2006 :
  http://rhn.redhat.com/errata/RHSA-2006-0573.html
- Bulletin de sécurité Mandriva MDKSA-2006:118 du 07 juillet 2006 :
  http://www.mandriva.com/security/advisories?name=MDKSA-2006:118
- Bulletin de sécurité Gentoo GLSA 200607-12 du 28 juillet 2006 :
  http://www.gentoo.org/security/en/glsa/glsa-200607-12.xml
- Bulletin de sécurité Debian DSA-1104 du 30 juin 2006 :
  http://www.us.debian.org/security/dsa-1104
- Bulletin de sécurité Ubuntu USN-313-1 du 11 juillet 2006 :
  http://www.ubuntu.com/usn/usn-313-1
- Bulletin de sécurité Ubuntu USN-313-2 du 19 juillet 2006 :
  http://www.ubuntu.com/usn/usn-313-2
- Bulletin de sécurité Suse du 03 juillet 2006 :
  http://lists.suse.com/archive/suse-security-announce/2006-Jul/0003.html
- Référence CVE CVE-2006-2198 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2198
- Référence CVE CVE-2006-2199 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2199
- Référence CVE CVE-2006-3117 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3117

Gestion détaillée du document

30 juin 2006 version initiale.

06 juillet 2006 ajout des références aux bulletins de sécurité Red Hat, Debian et Suse.

13 juillet 2006 ajout des références aux bulletins de sécurité d'Ubuntu.

04 août 2006 ajout des références aux bulletins de sécurité Gentoo, Mandriva et Ubuntu.