Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 octobre 2004
N° CERTA-2004-AVI-318-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité d'OpenOffice et StarOffice

Gestion du document

Référence	CERTA-2004-AVI-318-002
Titre	Vulnérabilité d'OpenOffice et StarOffice
Date de la première version	16 septembre 2004
Date de la dernière version	21 octobre 2004
Source(s)	Bulletin de sécurité SA12302 de Secunia
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

Atteinte à l'intégrité des données.

2 Systèmes affectés

- StarOffice 7 ;
- OpenOffice 1.1.2.

3 Description

OpenOffice et StarOffice sont deux suites bureautiques.

OpenOffice et StarOffice ne gèrent pas correctement les droits d'accès lors de la création des fichiers temporaires. Un utilisateur mal intentionné peut exploiter cette vulnérabilité pour accéder aux données d'un tiers.

4 Contournement provisoire

Positionner la variable d'environnement `$UMASK` permettant de positionner le droits d'accès par défaut ou positionner les variables d'environnement `$TMPDIR` vers un répertoire fils du répertoire `$HOME` de l'utilisateur.

5 Solution

Se référer aux différents bulletins de sécurité de l'éditeur pour l'obtention des correctifs (cf. section documentation).

6 Documentation

- Site d'OpenOffice :
  http://www.openoffice.org
- Correctif pour StarOffice (Solaris/x86) :
  http://sunsolve.sun.com/search/advsearch.do?collection=PATCH&type=collections&max=50&language=en&queryKey5=11
- Correctif pour StarOffice (Solaris/sparc) :
  http://sunsolve.sun.com/search/advsearch.do?collection=PATCH&type=collections&max=50&language=en&queryKey5=11
- Correctif pour StarOffice (Linux) :
  http://sunsolve.sun.com/search/advsearch.do?collection=PATCH&type=collections&max=50&language=en&queryKey5=11
- Bulletin de sécurité Secunia SA12302 du 13 septembre 2004 :
  http://secunia.com/advisories/12302
- Bulletin de sécurité Red Hat RHSA-2004:446 du 15 septembre 2004 :
  http://rhn.redhat.com/errata/RHSA-2004-446.html
- Bulletin de sécurité Mandrake MDKSA-2004:103 du 27 septembre 2004 :
  http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:103
- Bulletin de sécurité Gentoo GLSA-200410-17 du 20 octobre 2004 :
  http://www.gentoo.org/security/en/glsa/glsa-200410-17.xml
- Référence CVE CAN-2004-0752 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0752

Gestion détaillée du document

16 septembre 2004 version initiale.
29 septembre 2004 ajout référence au bulletin de sécurité de Mandrake.
21 octobre 2004 ajout référence au bulletin de sécurité de Gentoo.