

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans OpenOffice et LibreOffice

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-2012-AVI-285>

Gestion du document

Référence	CERTA-2012-AVI-285-001
Titre	Vulnérabilités dans OpenOffice et LibreOffice
Date de la première version	18 mai 2012
Date de la dernière version	22 mai 2012
Source(s)	Bulletin de sécurité OpenOffice et LibreOffice CVE-2012-1149 du 16 mai 2012 Bulletin de sécurité OpenOffice et LibreOffice CVE-2012-2334 du 16 mai 2012 Bulletin de sécurité OpenOffice CVE-2012-2149 du 16 mai 2012
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.

2 Systèmes affectés

- OpenOffice version 3.3, 3.4 Beta et antérieures ;
- libreOffice versions antérieures à la 3.5.3.

3 Résumé

Trois vulnérabilités ont été corrigées dans *OpenOffice* et deux dans *LibreOffice*. La première est un débordement d'entier dans « vclmi.dll » et provoque un débordement de mémoire tampon dans le tas. Une image JPEG spécialement conçue dans un fichier DOC peut être utilisée pour exploiter cette vulnérabilité. La deuxième concerne le format WPD et permet l'exécution de code arbitraire. La troisième ajoute des vérifications d'allocations mémoire lors de l'utilisation d'éléments graphiques dans un document de type POWERPOINT.

4 Solution

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

5 Documentation

- Bulletin de sécurité LibreOffice CVE-2012-1149 du 16 mai 2012 :
<http://www.libreoffice.org/advisories/cve-2012-1149/>
- Bulletin de sécurité LibreOffice CVE-2012-2334 du 16 mai 2012 :
<http://www.libreoffice.org/advisories/cve-2012-2334/>
- Bulletin de sécurité OpenOffice CVE-2012-1149 du 16 mai 2012 :
<http://www.openoffice.org/security/cves/CVE-2012-1149.html>
- Bulletin de sécurité OpenOffice CVE-2012-2149 du 16 mai 2012 :
<http://www.openoffice.org/security/cves/CVE-2012-2149.html>
- Bulletin de sécurité OpenOffice CVE-2012-2334 du 16 mai 2012 :
<http://www.openoffice.org/security/cves/CVE-2012-2334.html>
- Référence CVE CVE-2012-1149 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1149>
- Référence CVE CVE-2012-2149 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2149>
- Référence CVE CVE-2012-2334 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2334>

Gestion détaillée du document

18 mai 2012 version initiale.

22 mai 2012 Ajout de la vulnérabilité concernant la référence CVE CVE-2012-2334.