

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples Vulnérabilités dans IBM Lotus Notes

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-2007-AVI-459>

Gestion du document

Référence	CERTA-2007-AVI-459
Titre	Multiples Vulnérabilités dans IBM Lotus Notes
Date de la première version	26 octobre 2007
Date de la dernière version	–
Source(s)	Bulletins de sécurités IBM du 23 octobre 2007
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 à distance ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- IBM Lotus Notes 6.x ;
- IBM Lotus Notes 7.x.

3 Résumé

De multiples vulnérabilités sont présentes dans IBM Lotus Notes permettant à un utilisateur malintentionné distant de provoquer un déni de service, d'atteindre à la confidentialité des données ou d'exécuter du code arbitraire.

4 Description

Quatre vulnérabilités sont présentes dans le logiciel de messagerie Lotus Notes de IBM :

- la première est due à une erreur dans la mise en œuvre de visualiseurs externes de fichiers : `mifsr.dll`, `awsr.dll`, `kpagrdr.dll`, `exesr.dll`, `rtfsr.dll`, `mwsr.dll`, `wp6sr.dll`, `lsar.dll`. Cette faille peut être exploitée par le biais d'une pièce jointe construite de façon particulière et peut conduire à de l'exécution de code arbitraire à distance ;
- la seconde vulnérabilité est relative à une erreur dans la mise en œuvre des courriers au format HTML et peut conduire à de l'exécution de code arbitraire par le biais d'un courrier particulier ;
- la troisième est relative à une mauvaise gestion de la liste de contrôle d'exécution (ECL) et permet l'exécution d'une pièce jointe sans contrôle ou avertissement de l'application ;
- la dernière vulnérabilité concerne un manque de restrictions sur certaines zones de mémoire partagée et permet à un utilisateur local d'accéder aux données d'autres utilisateurs locaux.

5 Solution

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

6 Documentation

- Bulletin de sécurité IBM swg21271111 du 23 octobre 2007 :
<http://www-1.ibm.com/support/docview.wss?uid=swg21271111>
- Bulletin de sécurité IBM swg21272836 du 23 octobre 2007 :
<http://www-1.ibm.com/support/docview.wss?uid=swg21272836>
- Bulletin de sécurité IBM swg21272930 du 23 octobre 2007 :
<http://www-1.ibm.com/support/docview.wss?uid=swg21272930>
- Bulletin de sécurité IBM swg21270884 du 23 octobre 2007 :
<http://www-1.ibm.com/support/docview.wss?uid=swg21270884>
- Bulletin de sécurité IBM swg21257030 du 23 octobre 2007 :
<http://www-1.ibm.com/support/docview.wss?uid=swg21257030>
- Bulletin de sécurité IBM swg21271957 du 23 octobre 2007 :
<http://www-1.ibm.com/support/docview.wss?uid=swg21271957>
- Référence CVE CVE-2007-4222 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4222>
- Référence CVE CVE-2007-5544 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5544>

Gestion détaillée du document

26 octobre 2007 version initiale.