

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans IBM Lotus Domino

---

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-461>

---

### Gestion du document

Référence	CERTA-2007-AVI-461
Titre	Multiples vulnérabilités dans IBM Lotus Domino
Date de la première version	29 octobre 2007
Date de la dernière version	–
Source(s)	Bulletins de sécurité IBM
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 ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

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

## 3 Résumé

De multiples vulnérabilités dans Lotus Domino permettent à une personne malintentionnée d'exécuter du code arbitraire à distance ou de porter atteinte à la confidentialité des données.

## 4 Description

Quatre vulnérabilités ont été identifiées dans Lotus Domino :

- la première faille est un débordement de mémoire dans le module IMAP de Domino qui permet à une personne malintentionnée d'exécuter du code arbitraire à distance avec les privilèges du serveur ;

- la deuxième vulnérabilité est une erreur dans la méthode *Evaluate* de `LotusScript` qui peut provoquer la divulgation de données confidentielles ;
- la troisième vulnérabilité concerne un manque de restrictions dans les zones de mémoire partagée, ce qui peut permettre à un utilisateur local d'accéder aux données d'autres utilisateurs locaux ;
- la dernière faille concerne certaines commandes relatives à l'autorité de certification (*activate* et *unlock*) et peut résulter en l'affichage du mot de passe utilisé en clair.

## 5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation). Les versions 7.0.3 et 8.0 de Lotus Domino corrigent toutes les failles. Deux vulnérabilités ne sont pas corrigées dans les versions 6.x.

## 6 Documentation

- Bulletin de sécurité IBM swg21270623 du 23 octobre 2007 :  
<http://www-1.ibm.com/support/docview.wss?uid=swg21270623>
- Bulletin de sécurité IBM swg21261095 du 23 octobre 2007 :  
<http://www-1.ibm.com/support/docview.wss?uid=swg21261095>
- Bulletin de sécurité IBM swg21273266 du 24 octobre 2007 :  
<http://www-1.ibm.com/support/docview.wss?uid=swg21273266>
- Bulletin de sécurité IBM swg21257030 du 23 octobre 2007 :  
<http://www-1.ibm.com/support/docview.wss?uid=swg21257030>
- Référence CVE CVE-2007-3510 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3510>

## Gestion détaillée du document

**29 octobre 2007** version initiale.