



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 mars 2007
N° CERTA-2007-AVI-148

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-148>

Gestion du document

Référence	CERTA-2007-AVI-148
Titre	Multiples vulnérabilités dans IBM Lotus Domino
Date de la première version	28 mars 2007
Date de la dernière version	–
Source(s)	Bulletins de sécurité IBM du 27 mars 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

- Déni de service à distance ;
- injection de code indirecte (Cross Site Scripting).

2 Systèmes affectés

- IBM Lotus Domino 6.X ;
- IBM Lotus Domino 7.X ;
- IBM Lotus Web Access (Notes) 6.X ;
- IBM Lotus Web Access 7.X.

3 Résumé

De multiples vulnérabilités présentes dans IBM Lotus Domino permettent à un utilisateur distant de provoquer un déni de service ou de réaliser une attaque par injection de code indirecte (Cross-Site Scripting).

4 Description

Trois vulnérabilités sont présentes dans IBM Lotus Domino :

- la première de type débordement de tampon a été identifiée dans le service mettant en œuvre le protocole de messagerie IMAP ;
- la deuxième, également de type débordement de mémoire, concerne le serveur d'annuaire LDAP ;
- la dernière est due à un manque de contrôle de certains paramètres passés à l'application Lotus Domino Web Access.

Les deux premières vulnérabilités peuvent être utilisées par un utilisateur malveillant afin de provoquer un déni de service sur la machine vulnérable. Quant à la troisième, elle peut être exploitée pour réaliser une attaque de type Cross-Site Scripting.

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 swg21257026 du 27 mars 2007 :
<http://www.1-ibm.com/support/docview.wss?uid=swg21257026>
- Bulletin de sécurité IBM swg21257028 du 27 mars 2007 :
<http://www.1-ibm.com/support/docview.wss?uid=swg21257028>
- Bulletin de sécurité IBM swg21257248 du 27 mars 2007 :
<http://www.1-ibm.com/support/docview.wss?uid=swg21257248>

Gestion détaillée du document

28 mars 2007 version initiale.