

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans la gestion des clients sous 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-2001-AVI-024>

Gestion du document

Référence	CERTA-2001-AVI-024
Titre	Vulnérabilité dans la gestion des clients sous Lotus Notes
Date de la première version	01 mars 2001
Date de la dernière version	–
Source(s)	Avis de Lotus
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

Cette vulnérabilité des versions 4.6.x et 5.x du client Lotus Notes est indépendante du système exploitation.

3 Résumé

Un utilisateur mal intentionné peut, à l'aide d'un formulaire Lotus (*Stored Form*) habilement construit et inséré dans un courrier électronique, faire exécuter du code par le client de son destinataire.

4 Description

Le client Notes possède un outil permettant de faciliter l'affichage de données dans un courrier. Il permet de saisir les informations qui seront envoyées dans le document à partir d'un formulaire. Il est aussi possible d'envoyer ce formulaire au destinataire du message pour le cas où ce dernier ne le possède pas encore.

Il est possible d'insérer des scripts (LotusScript par exemple) dans ces formulaires. Selon son paramétrage le client risque d'exécuter le script automatiquement à la réception du courrier.

5 Contournement provisoire

Utiliser les ECL (*Execution Control List*) comme indiqué dans l'avis de sécurité de Lotus :

<http://www.notes.net/today.nsf/9148b29c86ffdc385256658007aaa0f3a9da544637a69b2852568310078b649?OpenDocument>

6 Documentation

Bulletin de sécurité de Lotus :

<http://support.lotus.com/sims2.nsf/eb5fbc0ab175cf0885256560005206cf/89e023ae7ee59e5d852569f90059fd5e?OpenDocument>

Gestion détaillée du document

01 mars 2001 version initiale.