Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 janvier 2001
N° CERTA-2001-AVI-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Lotus Domino 5

Gestion du document

Référence	CERTA-2001-AVI-001
Titre	Vulnérabilité de Lotus Domino 5
Date de la première version	12 janvier 2001
Date de la dernière version	–
Source(s)	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

- Accès à des données non-autorisées
- Exécution de code arbitraire.

2 Systèmes affectés

Vulnérabilité Lotus Domino 5.0 à 5.0.6 indépendante de la plate-forme.

3 Résumé

Une vulnérabilité de Lotus Domino 5 permet à un utilisateur mal intentionné d'avoir accès à distance en lecture à des fichiers qui ne lui sont pas normalement autorisés.

4 Description

Un utilisateur mal intentionné peut, par le biais d'une URL mal formée, accéder en lecture à tous les fichiers se situant sur le volume contenant les données du serveur web de Lotus Domino.

Le serveur HTTP de Domino a les privilèges du groupe d'utilisateurs *Système* (ou *system*), si ce volume est celui sur lequel est installé le système d'exploitation, l'intrus peut accéder à tous les fichiers systèmes.

5 Contournement provisoire

- Les données d'un serveur doivent toujours se situer sur un autre volume que le système en lui même.
- Le CERT-IST recommande d'effectuer une redirection de lien pour un élément de l'URL permettant l'accès à ces données non autorisées. Il s'agit de rediriger tout ce qui contient la chaîne de caractères `/../`.
  Pour cela :
  - Ouvrir le client d'administration du serveur,
  - sélectionner le serveur à administrer,
  - dans l'onglet *Configuration*, section *Serveur*, *Document serveur courant*,
  - cliquer sur le bouton *web...*,
  - sélectionner *Créer mappage/redirection d'URL*,
  - dans le document de redirection d'URL, onglet *Général*, Sélectionner *URL —>Redirection d'URL*,
  - dans l'onglet *mappage*, dans le champ *chemin d'URL entrante*, entrer : */../** et dans celui nommé *chaîne de redirection d'URL*, taper `http://nom du serveur/homepage.nsf` ou `homepage.nsf` est le nom de la page sur laquelle rediriger une tentative d'accès non-autorisé,
  - enregistrer le document et relancer la tâche HTTP (`tell HTTP restart`).

`Nota` **:** Pour supprimer cette redirection, il faut ouvrir le client d'administration, sélectionner le serveur à administrer, et dans l'onglet *configuration*, section *web*, *configuration de serveur web*, `supprimer` d'un clic droit sur la règle de redirection, puis relancer le service HTTP.

6 Solution

Appliquer le Correctif de Lotus dès qu'il paraît sur la liste des correctifs dont l'URL est indiquée dans la section `Documentation`.

7 Documentation

- L'avis de Lotus :
  http://www.lotus.com/developers/itcentral.nsf/F09A97EFEF47030F8525674B00574590/8AB14B289511F75F852569CF0078A512?OpenDocument
- la liste des correctifs de Lotus :
  http://www.notes.net/r5fixlist.nsf/SPRViewTemplate?OpenForm

Gestion détaillée du document

12 janvier 2001 version initiale.