Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 novembre 2001
N° CERTA-2001-AVI-141

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de Lotus domino Server 5.x

Gestion du document

Référence	CERTA-2001-AVI-141
Titre	Vulnérabilités de Lotus domino Server 5.x
Date de la première version	15 novembre 2001
Date de la dernière version	–
Source(s)	Bulletin de sécurité Lotus 189425 Bulletin de sécurité Lotus 189428 Bulletin de sécurité Lotus 189429
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

Lecture de données et exécution de programmes non autorisés.

2 Systèmes affectés

Serveurs Lotus Domino 5.x.

3 Résumé

En construisant habilement les URL dans un navigateur internet, il est possible d'obtenir un certain nombre d'informations concernant un serveur Domino et ses bases de données.

4 Description

Trois vulnérabilités différentes permettent d'obtenir des informations non autorisées sur des serveurs Lotus Domino 5.x :

1° Il est possible à un utilisateur sans privilège d'accéder à distance à l'un des fichiers servant à l'administration distante du serveur (*Web Administrator template file*), `webadmin.ntf`.

2° Lotus Domino possède une fonctionnalité appelée *Navigateur par Défaut* (`$DefaultNav`) permettant à un utilisateur de naviguer dans toute la base de données. Cette fonctionnalité ne devrait pas être accessible par des utilisateurs non autorisés. Un utilisateur mal intentionné peut accéder à des données non autorisées par le biais d'une URL habilement construite. Une première solution de contournement au moyen d'une redirection des URL `*/*.nsf/$DefaultNav*` avait été suggérée par Lotus. Mais elle n'est pas suffisante car elle peut être contournée.

3° Il est possible de présenter une base de données et ses documents sous la forme de *vues*. Des ACL (*Access Control List* correctement paramétrées permettent d'appliquer des permissions à certaines vues de façon à en empêcher l'accès à des utilisateurs spécifiés. Cependant, il est possible de contourner ces ACL par le biais d'une URL habilement construite utilisant une autre vue ayant des contrôles d'accès plus laxistes, pour visualiser un document non autorisé.

5 Contournement provisoire

1° Pour la vulnérabilité de `webadmin.ntf`, Lotus recommande d'utiliser le client `Domino Designer` afin de modifier les ACL qui sont appliquées à ce fichier. Si nécessaire, changer le niveau de sécurité par défaut à `No Access`.

2° Pour la vulnérabilité concernant l'accès à la base de données complète par un utilisateur sans privilège, Lotus recommande de modifier les permissions document par document afin que les documents ne soient pas accessibles par des utilisateurs non autorisés.

3° Pour la vulnérabilité concernant l'accès aux données par le biais de `vues` détournées, Lotus recommande d'appliquer des permissions spécifiques à chaque document au moyen de son champ `lecture`.

6 Solution

1° La version 5.0.9 de Domino corrige les permissions d'accès par défaut au fichier `webadmin.ntf`.
Attention ! Si l'administrateur crée lui-même des fichiers permettant d'administrer à distance des bases de données, il doit y appliquer les ACL nécessaires pour que ceux-ci ne soient pas utilisables par un utilisateur sans privilège (de la même façon que l'on applique des permissions particulières aux scripts *cgi* d'un serveur web).

2° La version 5.0.10 corrige les permissions et supprime l'accès à la base de données par le biais de la fonctionalité de *Navigateur par Défaut*.

7 Documentation

1° Concernant la première vulnérabilité :
Avis 189425 :
http://support.lotus.com/sims2.nsf/0/7ee0d1a8ec05c3bb85256afc005ae0ea

2° Concernant la seconde vulnérabilité :

- Avis 189428 :
  http://support.lotus.com/sims2.nsf/0/4f4044be36ed537885256afc0063975c
- Document Lotus : *A guide to Secure Domino App* :
  http://support.lotus.com/sims2.nsf/e9f368754034a5cc852563ab006d15a3/00a9f62432c46b018525683b0066e579?OpenDocument
- Document Lotus : *White Paper : A guide to Developping Secure Domino App* :
  http://www.lotus.com/developers/itcentral.nsf/wdocs/74070EA8E6B8DAC8852568320061FA74
- Document de Lotus : *Designing a Secure Domino App* :
  http://www.notes.net/today.nsf/8a6d147cf55a7fd385256658007aacf1/71102330e24a7ce5852564b5005e3682?OpenDocument

3° Concernant la troisième vulnérabilité :

- Avis 189429 :
  http://support.lotus.com/sims2.nsf/0/73013cc3db3a280685256afc006560be
- Document de Lotus : *The ABCs of using the ACL* :
  http://www.notes.net/today.nsf/8a6d147cf55a7fd385256658007aacf1/be08e4acfc72cd72852565d9004cb61c
- Document de Lotus : *Designing a Secure Domino App* :
  http://www.notes.net/today.nsf/8a6d147cf55a7fd385256658007aacf1/71102330e24a7ce5852564b5005e3682?OpenDocument

Gestion détaillée du document

15 novembre 2001 version initiale.