Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 6 décembre 2000
N° CERTA-2000-AVI-084

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités des serveurs Lotus Domino

Gestion du document

Référence	CERTA-2000-AVI-084
Titre	Vulnérabilités des serveurs Lotus Domino
Date de la première version	6 décembre 2000
Date de la dernière version	–
Source(s)	Première partie vérifiée au CERTA Seconde partie 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

- Déni de service SMTP et exécution potentielle de code arbitraire;
- accès à des données non autorisées;
- augmentation des privilèges.

2 Systèmes affectés

Tout système possédant le service SMTP de Lotus Domino en fonction.
Toute version de Domino inférieure ou égale à 5.0.4

3 Résumé

3.1 Déni de service de messagerie

Il est possible de bloquer à distance le service SMTP d'un serveur Domino par un débordement de pile.

3.2 Autres vulnérabilités

Par ailleurs, de nombreuses autres vulnérabilités sont largement diffusées et exploitées sur internet.

4 Description

4.1 Déni de service de messagerie

Un utilisateur mal intentionné peut bloquer à distance le service SMTP d'un serveur Domino par un débordement de pile, en envoyant un courrier internet habilement conçu. Il faut savoir que la plupart des débordements de pile permettent l'exécution de code arbitraire sur la machine vulnérable, s'il sont habilement réalisés.

4.2 Autres vulnérabilités

D'autre part il existe d'autres vulnérabilités dans les serveurs Domino de version inférieure ou égale à 5.0.2 : l'utilisation des paramètres par défaut, sans vérification par l'administrateur, lors de l'installation du serveur Domino, en sont la principale cause. Les ACL (*Access Control List* : liste des privilèges d'accès) par défaut des bases de données d'origine (*names.nsf*, *catalog.nsf*, *domcfg.nsf* et *log.nsf*) sont laxistes. Il est, entre autres choses, possible parcourir ces bases avec un simple navigateur internet, ou de modifier la configuration du serveur si les paramétrages par défaut n'ont pas été revus. Il est aussi possible de retrouver les mots de passe utilisateurs à partir du hachage obtenu par une authentification lors d'un accès par un navigateur.

5 Contournement provisoire

Il n'y a pas de contournement provisoire pour le service SMTP.

Revoir les paramètres d'installation de Domino, et renforcer les ACL et les ECL (*extended control list* complément des ACL).

6 Solution

Mettre à jour Lotus domino dans sa version 5.0.5 :

- Pour Windows 9x ou NT :
  - domino server première partie :
    http://http2.notes.net/pub/504a_505/w32nsrvg.exe
  - domino server seconde partie :
    http://http2.notes.net/pub/504a_505/dols_w32n.exe
- Pour Windows NT, processeur Alpha :
  http://http2.notes.net/pub/504a_505/w32asrvg.exe
- Pour Sun Solaris :
  - processeur Sparc :
    http://http2.notes.net/pub/504a_505/sunssrvg.tar
  - processeur Intel :
    http://http2.notes.net/pub/504a_505/sunisrvg.tar
- OS2 :
  - Domino première partie :
    http://http2.notes.net/pub/504a_505/os2srvg.exe
  - Domino server seconde partie :
    http://http2.notes.net/pub/504a_505/dols_os2.exe
- Macintosh PPC :
  http://http2.notes.net/pub/504a_505/504a505designer.hqx

- Linux :
  http://http2.notes.net/pub/504a_505/lnxsrvg.tar
- IBM AIX :
  http://http2.notes.net/pub/504a_505/aixsrvg.tar
- HP-UX :
  http://http2.notes.net/pub/504a_505/hpuxsrvg.tar

Vérifier si la configuration par défaut est compatible avec votre politique de sécurité après toute installation ou mise à jour.

7 Documentation

Pour la deuxième partie de cet avis, consulter le site de Lotus :
http://www.lotus.com/developers/itcentral.nsf/wdocs/C52C07308269989B8525692D008322BD
http://www.lotus.com/home.nsf/welcome/securityzone

Gestion détaillée du document

6 décembre 2000 version initiale.