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 2003
N° CERTA-2003-AVI-068

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Deux vulnérabilités de Lotus Notes et Domino

Gestion du document

Référence	CERTA-2003-AVI-068
Titre	Deux vulnérabilités de Lotus Notes et Domino
Date de la première version	28 mars 2003
Date de la dernière version	–
Source(s)	Avis CA-2003-11 du CERT/CC
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 ;
- déni de service.

2 Systèmes affectés

- Lotus Notes et Domino versions 5.0.12, 6.0.1 et antérieures ;
- Lotus Domino 6.0 versions alpha et beta.

3 Résumé

Deux vulnérabilités de Lotus Notes et Domino permettent à un utilisateur mal intentionné d'exécuter du code arbitraire ou de provoquer un déni de service.

4 Description

La première vulnérabilité concerne un débordement de mémoire dans le service *COM Object Control Handler* de Lotus Notes et Domino.

Cette vulnérabilité avait été annoncée comme une vulnérabilité de iNotes ActiveX, mais elle n'est pas spécifique à iNotes ou aux ActiveX. Elle peut notamment être présente sur des clients Notes ou des serveurs Domino installés sur d'autres plates-formes que Microsoft Windows.

Les systèmes affectés sont Lotus Notes et Domino versions 5.0.12, 6.0.1 et antérieures.

La deuxième vulnérabilité concerne le protocole LDAP. Les versions de Lotus Domino R5.0.7 et antérieures présentaient une vulnérabilité dans la gestion du protocole LDAP, qui avait été corrigée dans la version R5.0.7a.

Cette vulnérabilité est à nouveau présente dans les versions Lotus Notes et Domino R6 alpha et beta.

5 Solution

Appliquer le correctif pour la première vulnérabilité.

Les versions Lotus Domino et Notes R6.0 Gold et R6.0.1 corrigent la deuxième vulnérabilité.

6 Documentation

- Avis CA-2003-11 du CERT/CC :
  http://www.cert.org/advisories/CA-2003-11.html

- Avis de sécurité IBM (première vulnérabilité) :
  http://www-1.ibm.com/support/docview.wss?uid=swg21104543

- Avis de sécurité NGSSoftware Insight NISR17022003e (première vulnérabilité) :
  http://www.nextgenss.com/advisories/lotus-inotesclientaxbo.txt

- Avis R7-0012 de Rapid7 (deuxième vulnérabilité) :
  http://www.rapid7.com/advisories/R7-0012.html

- Référence CVE (deuxième vulnérabilité) :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-1311

Gestion détaillée du document

28 mars 2003 version initiale.