

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité sur le protocole d'authentification de 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-2003-AVI-049>

---

### Gestion du document

Référence	CERTA-2003-AVI-049
Titre	Vulnérabilité sur le protocole d'authentification de Lotus Notes
Date de la première version	17 mars 2003
Date de la dernière version	-
Source(s)	Avis VU#433489 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

- Déni de service ;
- exécution de code arbitraire.

## 2 Systèmes affectés

- Lotus Notes R4 ;
- Lotus Notes R5 versions antérieures à la version R5.0.11 ;
- Lotus Notes R6 versions betas et pré-version.

## 3 Résumé

Une vulnérabilité du procédé d'authentification des utilisateurs sur un serveur Lotus Domino permet à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire sur le système.

## 4 Description

Lorsqu'un client désire se connecter à un serveur Lotus Notes, il est nécessaire qu'il s'authentifie auprès de se serveur. Cette authentification consiste en une série d'échanges entre le client et le serveur (mode « challenge / réponse ») afin d'authentifier l'utilisateur.

Une vulnérabilité présente dans cette authentification permet à un utilisateur mal intentionné, par le biais de paquets malicieusement écrits, de réaliser un déni de service ou d'exécuter du code arbitraire sur le serveur.

## 5 Solution

Appliquer le correctif correspondant à votre version de Lotus Notes (cf. section documentation).

Notes : Les versions R5.0.12, R6.0 Gold et R6.0.1 des serveurs Lotus Notes ne sont pas vulnérables.

## 6 Documentation

- Avis du CERT/CC :  
<http://www.kb.cert.org/vuls/id/433489>
- Avis de sécurité TN 1105060 de Lotus Notes :  
<http://www-1.ibm.com/support/docview.wss?rs=463&uid=swg21105101>
- Référence CVE :  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0122>
- Correctif :  
<http://www-10.lotus.com/ldd/r5fixlist.nsf>

## Gestion détaillée du document

17 mars 2003 version initiale.