



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 25 juin 2004  
N° CERTA-2004-AVI-207

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité du client 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-2004-AVI-207>

---

### Gestion du document

Référence	CERTA-2004-AVI-207
Titre	Vulnérabilité du client Lotus Notes
Date de la première version	25 juin 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité 06.23.04 d'iDEFENSE
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 à distance.

## 2 Systèmes affectés

Lotus Notes 6.5.x, 6.0.x

## 3 Description

Le client Lotus Notes ne filtre pas correctement les caractères spéciaux contenus dans les URL de la forme `notes://`.

En incitant un utilisateur à visualiser au moyen d'un client Lotus Notes une page HTML habilement constituée, un utilisateur mal intentionné peut forcer l'exécution de code arbitraire à distance sur la plate-forme vulnérable.

## 4 Solution

Les versions 6.0.4 et 6.5.2 corrigent cette vulnérabilité.

## **5 Documentation**

- Bulletin de sécurité 06.23.04 d'iDEFENSE :  
<http://www.idefense.com/application/poi/display?id=111&type=vulnerabilities>
- Bulletin de sécurité "Lotus Notes URL handler argument injection vulnerability" d'IBM :  
<http://www-1.ibm.com/support/docview.wss?rs=463&uid=swg21169510>
- Référence CVE CAN-2004-0480 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0480>

### **Gestion détaillée du document**

**25 juin 2004** version initiale.