



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 12 février 2008  
N° CERTA-2008-AVI-070

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans UltraVNC

---

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-2008-AVI-070>

---

### Gestion du document

Référence	CERTA-2008-AVI-070
Titre	Multiples vulnérabilités dans UltraVNC
Date de la première version	12 février 2008
Date de la dernière version	–
Source(s)	
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

*UltraVNC*, version 1.0.2 et 1.0.4RC.

## 3 Résumé

Des vulnérabilités dans le module *vncviewer* du logiciel *UltraVNC* permettent à un utilisateur malveillant d'exécuter du code arbitraire à distance.

## 4 Description

*UltraVNC* est un logiciel qui permet d'utiliser un ordinateur distant.

Des fonctions dans *vncviewer/FileTransfer.cpp* présentent plusieurs défauts de vérification de longueur de données. Ces défauts sont exploitables par un utilisateur malveillant pour exécuter sur le système vulnérable un code

arbitraire à distance. Pour que cette exploitation de vulnérabilité réussisse, le système vulnérable doit exécuter *vncviewer* en écoute (*listening mode*).

L'exploitation au travers du greffon *DSM* est également possible si l'utilisateur malveillant connaît la clé de chiffrement utilisée par *vncviewer*.

Le module *UltraVNC Server* ne serait pas vulnérable.

## **5 Solution**

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## **6 Documentation**

- Bulletin UltraVNC du 08 février 2008 :  
<http://forum.ultravnc.info/viewtopic.php?p=45150>
- Site de téléchargement UltraVNC :  
<http://www.uvnc.com/>

## **Gestion détaillée du document**

**12 février 2008** version initiale.