

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité d'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-042>

Gestion du document

Référence	CERTA-2008-AVI-042-001
Titre	Vulnérabilité d'UltraVNC
Date de la première version	04 février 2008
Date de la dernière version	06 février 2008
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, versions 1.0.2 et 1.0.4RC.

3 Résumé

Une vulnérabilité dans le module *vncviewer* du logiciel *UltraVNC* permet à un utilisateur malveillant d'exécuter du code arbitraire à distance sur le système vulnérable.

4 Description

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

Une fonction dans *vncviewer/ClientConnection.cpp* présente un défaut de vérification de longueur de données. Ce défaut est exploitable 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 utilisé par *vncviewer*.

Le module *UltraVNC Server* ne serait pas vulnérable.

5 Solution

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

6 Documentation

- Bulletin UltraVNC du 25 janvier 2008 :
<http://forum.ultravnc.info/viewtopic.php?t=11850>
- Site de téléchargement UltraVNC :
<http://www.uvnc.com/>
- Discussions dans le forum UltraVNC :
<http://forum.ultravnc.info/viewtopic.php?t=11850>
- Référence CVE CVE-2008-0610 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0610>

Gestion détaillée du document

04 février 2008 version initiale.

06 février 2008 ajout de la référence au CVE associé.