

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans rdesktop

---

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-322>

---

### Gestion du document

|                             |                                        |
|-----------------------------|----------------------------------------|
| Référence                   | CERTA-2008-AVI-322                     |
| Titre                       | Vulnérabilité dans rdesktop            |
| Date de la première version | 17 juin 2008                           |
| Date de la dernière version | –                                      |
| Source(s)                   | Bulletin de mise à jour du 10 mai 2008 |
| 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 ;
- déni de service à distance.

## 2 Systèmes affectés

*rdesktop* version 1.5 et antérieures

## 3 Résumé

Une vulnérabilité permettant l'exécution de code arbitraire affecte *rdesktop* lors du traitement des requêtes RDP.

## 4 Description

*rdesktop* est un client permettant aux utilisateurs de systèmes de type Unix de se connecter au *Windows Terminal Server* et d'accéder graphiquement et à distance à leur bureau Windows. La vulnérabilité, de type débordement de mémoire, affecte une fonction utilisée pour le traitement des requêtes RDP.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité Debian DSA 1573 du 11 mai 2008 :  
<http://www.debian.org/security/2008/dsa-1573>
- Mise à jour de sécurité Fedora Core 3886 du 14 mai 2008 :  
<http://www.redhat.com/archives/fedora-package-announce/2008-May/msg00244.html>
- Mise à jour de sécurité Fedora Core 3917 du 14 mai 2008 :  
<http://www.redhat.com/archives/fedora-package-announce/2008-May/msg00270.html>
- Mise à jour de sécurité Fedora Core 3985 du 14 mai 2008 :  
<http://www.redhat.com/archives/fedora-package-announce/2008-May/msg00296.html>
- Bulletin de sécurité Mandriva MDVSA-2008:101 du 16 mai 2008 :  
<http://www.mandriva.com/archives/security/advisories>
- Bulletin de sécurité iDefense 696 du 07 mai 2008 :  
<http://www.ideo.com/ntelligence/vulnerabilities/display.php?id=696>
- Référence CVE CVE-2008-1801 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1801>
- Référence CVE CVE-2008-1802 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1802>
- Référence CVE CVE-2008-1803 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1803>

## Gestion détaillée du document

**17 juin 2008** version initiale.