

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans Kerberos

---

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-2007-AVI-019>

---

### Gestion du document

Référence	CERTA-2007-AVI-019
Titre	Vulnérabilités dans Kerberos
Date de la première version	10 janvier 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité MIT MITKRB5-SA-2006-002 du 09 janvier 2007 Bulletin de sécurité MIT MITKRB5-SA-2006-003 du 09 janvier 2007
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

- kadmind versions krb5-1.4 à krb5-1.4.4 ;
- kadmind versions krb5-1.5 à krb5-1.5.1 ;
- toute application tiers utilisant les bibliothèques GSS-API et RPC incluses dans les versions krb5-1.4 à krb5-1.4.4 et krb5-1.5 à krb5-1.5.1.

Les versions de kadmind antérieures à krb5-1.4 ne sont pas affectées.

## 3 Résumé

Deux vulnérabilités découvertes dans kadmind permettent l'exécution de code arbitraire à distance.

## 4 Description

Deux vulnérabilités ont été découvertes dans `kadmind`.

La première est présente dans la partie serveur de la bibliothèque `RPC`. La seconde résulte de problèmes de gestion de la mémoire dans l'interface `mechglue` de la bibliothèque `GSS-API`. Un utilisateur malintentionné peut exploiter l'une de ces vulnérabilités, sans authentification préalable, pour exécuter du code arbitraire à distance.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité MIT MITKRB5-SA-2006-002 du 09 janvier 2007 :  
<http://web.mit.edu/kerberos/advisories/MITKRB-SA-2006-002-rpc.txt>
- Bulletin de sécurité MIT MITKRB5-SA-2006-003 du 09 janvier 2007 :  
<http://web.mit.edu/kerberos/advisories/MITKRB-SA-2006-003-mechglue.txt>
- Référence CVE CVE-2006-6143 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6143>
- Référence CVE CVE-2006-6144 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6144>

## Gestion détaillée du document

**10 janvier 2007** version initiale.