

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de MIT Kerberos 5

---

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-2005-AVI-257>

---

### Gestion du document

Référence	CERTA-2005-AVI-257-005
Titre	Vulnérabilité de MIT Kerberos 5
Date de la première version	13 juillet 2005
Date de la dernière version	03 octobre 2006
Source(s)	Bulletins de sécurité MITKRB5-SA-2005-002 et MITKRB5-SA-2005-003
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

- Déni de service ;
- exécution de code arbitraire à distance.

## 2 Systèmes affectés

MIT Kerberos 5 version krb5-1.4.1 et versions antérieures.

## 3 Résumé

Plusieurs vulnérabilités dans MIT Kerberos 5 permettent à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire à distance sur la plate-forme vulnérable.

## 4 Description

Kerberos est un protocole d'authentification.

Plusieurs vulnérabilités ont été découvertes dans MIT Kerberos 5 :

- Une vulnérabilité au niveau du KDC (Key Distribution Center) dans la gestion de la mémoire lors de la réception d'un paquet TCP habilement construit (référence CVE CAN-2005-1174) ;

- une vulnérabilité au niveau du KDC (Key Distribution Center) de type débordement de mémoire lors de la réception d'un paquet TCP ou UDP habilement construit (référence CVE CAN-2005-1175) ;
- une vulnérabilité dans la gestion de la mémoire par la fonction `krb5_recvauth()` (référence CVE CAN-2005-1689).

## 5 Solution

La future version `krb5-1.4.2` corrigera ces vulnérabilités.

En attendant, appliquer les correctifs pour la version `krb5-1.4.1` :

- [http://web.mit.edu/kerberos/advisories/2005-002-patch\\_1.4.1.txt](http://web.mit.edu/kerberos/advisories/2005-002-patch_1.4.1.txt)
- [http://web.mit.edu/kerberos/advisories/2005-003-patch\\_1.4.1.txt](http://web.mit.edu/kerberos/advisories/2005-003-patch_1.4.1.txt)

MIT Kerberos 5 peut se télécharger à l'adresse suivante :

<http://web.mit.edu/kerberos/dist/index.html>

Dans tous les cas, se référer au bulletin de sécurité de l'éditeur (cf. section Documentation) pour l'obtention des correctifs.

## 6 Documentation

- Site Internet de MIT Kerberos 5 :  
<http://web.mit.edu/kerberos/>
- Bulletin de sécurité MITKRB5-SA-2005-002 du 12 juillet 2005 :  
<http://web.mit.edu/kerberos/advisories/MITKRB5-SA-2005-002-kdc.txt>
- Bulletin de sécurité MITKRB5-SA-2005-003 du 12 juillet 2005 :  
<http://web.mit.edu/kerberos/advisories/MITKRB5-SA-2005-003-recvauth.txt>
- Bulletin de sécurité Gentoo GLSA 200507-11 du 12 juillet 2005 :  
<http://www.gentoo.org/security/en/glsa/glsa-200507-11.xml>
- Bulletin de sécurité RedHat RHSA-2005:562 du 12 juillet 2005 :  
<http://rhn.redhat.com/errata/RHSA-2005-562.html>
- Bulletin de sécurité RedHat RHSA-2005:567 du 12 juillet 2005 :  
<http://rhn.redhat.com/errata/RHSA-2005-567.html>
- Bulletin de sécurité SUN #101809 du 12 juillet 2005 :  
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-101809-1>
- Bulletin de sécurité SUN #101810 du 12 juillet 2005 :  
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-101810-1>
- Bulletin de sécurité SUSE SUSE-SR:2005:017 du 13 juillet 2005 :  
[http://www.novell.com/linux/security/advisories/2005\\_17\\_sr.html](http://www.novell.com/linux/security/advisories/2005_17_sr.html)
- Bulletin de sécurité Mandriva MDKSA-2005:119 du 13 juillet 2005 :  
<http://www.mandriva.com/security/advisories?name=MDKSA-2005:119>
- Bulletin de sécurité Debian DSA-757 du 17 juillet 2005 :  
<http://www.debian.org/security/2005/dsa-757>
- Bulletin de sécurité SGI 20050703-01-U du 15 juillet 2005 :  
<ftp://patches.sgi.com/support/free/security/advisories/20050703-01-U.asc>
- Bulletin de sécurité HP-UX du 25 septembre 2006:  
<http://itrc.hp.com/service/cki/docDisplay.do?docId=c00768776>
- Référence CVE CAN-2005-1174 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1174>
- Référence CVE CAN-2005-1175 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1175>
- Référence CVE CAN-2005-1689 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1689>

## **Gestion détaillée du document**

**13 juillet 2005** version initiale.

**13 juillet 2005** ajout de la référence au bulletin de sécurité SUSE SUSE-SR:2005:017.

**15 juillet 2005** ajout de la référence au bulletin de sécurité Mandriva MDKSA-2005:119.

**18 juillet 2005** ajout de la référence au bulletin de sécurité Debian DSA-757.

**18 juillet 2005** ajout des références aux bulletins de sécurité RedHat RHSA-2005:562 et SGI 20050703-01-U.

**03 octobre 2006** ajout de la référence au bulletin de sécurité HP-UX