

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Plusieurs vulnérabilités dans MIT Kerberos krb5

---

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-2006-AVI-356>

---

### Gestion du document

Référence	CERTA-2006-AVI-356-001
Titre	Plusieurs vulnérabilités dans MIT Kerberos krb5
Date de la première version	16 août 2006
Date de la dernière version	18 août 2006
Source(s)	Bulletin de sécurité MITKRB5-SA-2006-001 du 08 août 2006
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

- Contournement de la politique de sécurité ;
- élévation de privilèges.

## 2 Systèmes affectés

La version 1.5 et 1.4.3 ainsi que celles antérieures.

## 3 Description

Kerberos est un protocole d'authentification créé par le MIT. Il fonctionne sur le principe de tickets donnant différents droits d'accès (période de validité, services accordés, etc). L'implémentation la plus fréquente est la version 5 du MIT, nommée `krb5`.

Plusieurs vulnérabilités ont été identifiées dans ce dernier. Sous certaines conditions, différentes applications fournies avec `krb5` (`krshd`, `v4rcp`, `ftpd`, `ksu`) ne contrôlèrent pas de manière suffisamment rigoureuse les appels aux fonctions système `setuid()` et `seteuid()`. Ces dernières fixent les propriétés `UIDs/GIDs` (pour *User/Group IDs*) d'un processus. Un utilisateur malveillant local au système pourrait exploiter ces vulnérabilités pour élever ses privilèges à ceux d'administrateur (`root`) et exécuter des commandes arbitraires sur le système.

## 4 Solution

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

## 5 Documentation

- Page du projet MIT Kerberos Version 5 krb5 :  
<http://web.mit.edu/Kerberos/>
- Bulletin de sécurité MITKRB5-SA-2006-001 du 08 août 2006 :  
<http://web.mit.edu/Kerberos/advisories/MITKRB5-SA-2006-001-setuid.txt>
- Mise à jour proposée par le MIT pour les versions 1.5 de Kerberos krb5 du 08 août 2006 :  
[http://web.mit.edu/Kerberos/advisories/2006-001-patch\\_1.5.txt](http://web.mit.edu/Kerberos/advisories/2006-001-patch_1.5.txt)
- Mise à jour proposée par le MIT pour les versions 1.4.3 de Kerberos krb5 du 08 août 2006 :  
[http://web.mit.edu/Kerberos/advisories/2006-001-patch\\_1.4.3.txt](http://web.mit.edu/Kerberos/advisories/2006-001-patch_1.4.3.txt)
- Référence CVE CVE-2006-3083 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3083>
- Référence CVE CVE-2006-3084 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3084>
- Bulletin de sécurité Ubuntu USN-334-1 du 16 août 2006 :  
<http://www.ubuntu.com/usn/usn-334-1>
- Bulletin de sécurité Debian DSA 1146-1 du 09 août 2006 :  
<http://www.debian.org/security/2006/dsa-1146>
- Mise à jour Fedora FEDORA-2006-905 du 09 août 2006 :  
<http://www.redhat.com/archives/fedora-package-announce/2006-August/msg00023.html>  
<http://download.fedora.redhat.com/pub/fedora/linux/core/updates/5/>
- Bulletin de sécurité RedHat RHSA-2006:0612-8 du 08 août 2006 :  
<http://rhn.redhat.com/errata/RHSA-2006-0612.html>
- Bulletin de sécurité Mandriva MDKSA-2006:139 du 09 août 2006 :  
<http://www.mandriva.com/security/advisories?name=MDKSA-2006:139>

## Gestion détaillée du document

**16 août 2006** version initiale.

**18 août 2006** ajout des bulletins de sécurité Ubuntu, Debian, Fedora, RedHat et Mandriva.