

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans MIT 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-2011-AVI-078>

---

### Gestion du document

Référence	CERTA-2011-AVI-078-001
Titre	Vulnérabilités dans MIT Kerberos
Date de la première version	10 février 2011
Date de la dernière version	16 février 2011
Source(s)	Bulletin de sécurité Kerberos MITKRB5-SA-2011-001 du 08 février 2011 Bulletin de sécurité Kerberos MITKRB5-SA-2011-002 du 08 février 2011
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 à distance.

## 2 Systèmes affectés

MIT Kerberos 5-1.6 à 5-1.9.

## 3 Résumé

Plusieurs vulnérabilités dans Kerberos permettent à un utilisateur malveillant de provoquer un déni de service à distance.

## 4 Description

Plusieurs vulnérabilités sont présentes dans Kerberos :

- (CVE-2010-4022, versions 5-1.7 à 5-1.9) le processus démon *kproxd* traite de manière incorrecte des entrées réseau invalides. Cela peut provoquer l'arrêt de ce processus et celui de son processus père, bloquant la propagation des mises à jour en provenance du KDC (*Key distribution centre*) maître ;

- (CVE-2011-0281, versions 5-1.6 à 5-1.9) l'interrogation d'un annuaire LDAP, quand ce procédé est utilisé par Kerberos, contient un défaut qui est exploitable au moyen d'une requête particulière pour empêcher les communications entre le KDC et l'annuaire ;
- (CVE-2011-0282, versions 5-1.6 à 5-1.9) quand Kerberos utilise un annuaire LDAP, certaines recherches provoquent un arrêt inopiné du serveur, exploitable au moyen d'une requête spécialement conçue ;
- (CVE-2011-0283, version 5-1.9) un paquet malformé peut provoquer un arrêt inopiné du serveur.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité Kerberos MITKRB5-SA-2011-001 du 08 février 2011 :  
<http://web.mit.edu/kerberos/advisories/MITKRB5-SA-2011-001.txt>
- Bulletin de sécurité Kerberos MITKRB5-SA-2011-002 du 08 février 2011 :  
<http://web.mit.edu/kerberos/advisories/MITKRB5-SA-2011-002.txt>
- Bulletin de sécurité RedHat RHSA-2011:0199-1 du 08 février 2011 :  
<http://rhn.redhat.com/errata/RHSA-2011-0199.html>
- Bulletin de sécurité Ubuntu USN-1062-1 du 15 février 2011 :  
<http://www.ubuntu.com/usn/usn-1062-1>
- Référence CVE CVE-2010-4022 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4022>
- Référence CVE CVE-2011-0281 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0281>
- Référence CVE CVE-2011-0282 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0282>
- Référence CVE CVE-2011-0283 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0283>

## Gestion détaillée du document

**10 février 2011** version initiale.

**16 février 2011** ajout des références aux bulletins RedHat et Ubuntu et rectification des CVE.