

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans pam\_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-2008-AVI-484>

---

### Gestion du document

Référence	CERTA-2008-AVI-484
Titre	Vulnérabilité dans pam_krb5
Date de la première version	07 octobre 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité RedHat RHSA-2008:0907 du 02 octobre 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

Contournement de la politique de sécurité.

## 2 Systèmes affectés

– pam\_krb5 versions antérieures à 2.3.2-1.

## 3 Description

Une vulnérabilité découverte dans pam\_krb5 permet à un utilisateur local de contourner la politique de sécurité.

Cette vulnérabilité peut-être exploitée par une personne malveillante afin de changer de compte d'utilisateur en affectant une valeur spécifique à la variable KRB5CCNAME.

L'option `existing_ticket` doit être activée afin de rendre la vulnérabilité exploitable.

## 4 Solution

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

## **5 Documentation**

- Bulletin de sécurité RedHat RHSA-2008:0907 du 02 octobre 2008 :  
<http://rhn.redhat.com/errata/RHSA-2008-0907.html>
- Référence CVE CVE-2008-3825 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3825>

### **Gestion détaillée du document**

**07 octobre 2008** version initiale.