

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité 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-2010-AVI-476>

Gestion du document

Référence	CERTA-2010-AVI-476
Titre	Vulnérabilité dans MIT Kerberos
Date de la première version	07 octobre 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité MITKRB5-SA-2010-006 du 05 octobre 2010
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

- Dénis de service à distance ;
- exécution de code arbitraire à distance ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

MIT krb5-1.8 à MIT krb5-1.8.3

3 Résumé

MIT Kerberos présente une vulnérabilité permettant à un utilisateur distant d'effectuer un déni de service, de porter atteinte à la confidentialité des données ou d'exécuter du code arbitraire.

4 Description

Une vulnérabilité de type déréréférencement de pointeur nul est présente dans MIT Kerberos. Elle concerne le KDC (Key Distribution Center). Elle peut être exploitée par le biais d'un certain type de message

envoyé depuis le TGS (Ticket Granting Server). Cette vulnérabilité peut entraîner un déni de service, une exécution de code à distance ou porter atteinte à la confidentialité des données.

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 Kerberos MITKRB5-SA-2010-006 :
<http://web.mit.edu/kerberos/advisories/MITKRB5-SA-2010-006.txt>
- Référence CVE CVE-2010-1322 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1322>

Gestion détaillée du document

07 octobre 2010 version initiale.