

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-2011-AVI-155>

Gestion du document

Référence	CERTA-2011-AVI-155
Titre	Vulnérabilité dans MIT Kerberos
Date de la première version	16 mars 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Kerberos MITKRB5-SA-2011-003 du 15 mars 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

- Exécution de code arbitraire à distance ;
- déni de service à distance.

2 Systèmes affectés

MIT Kerberos 5.1-7, 5.1-8 et 5.1-9.
Des extensions développées par des tiers peuvent être vulnérables.

3 Résumé

Une vulnérabilité sur certaines configurations de MIT Kerberos permet à un utilisateur malveillant de provoquer un déni de service à distance. L'exécution de code arbitraire à distance est possible.

4 Description

Le service de MIT Kerberos KDC (*Key Distribution Center*) configuré pour répondre aux requêtes PKINIT (*Public Key Cryptography for Initial Authentication*) est vulnérable à une double libération de mémoire. L'exploitation de cette erreur permet à un utilisateur malveillant de provoquer un arrêt inopiné du serveur.

L'exécution de code arbitraire à distance est considérée par l'éditeur comme difficile, mais possible.

Des extensions développées par des tiers peuvent être vulnérables lorsqu'elles écrivent des données TYPED-DATA dans le champ e-data des messages KRB-ERROR.

5 Solution

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

6 Documentation

- Bulletin de sécurité Kerberos MITKRB5-SA-2011-003 du 15 mars 2011 :
<http://web.mit.edu/kerberos/advisories/MITKRB5-SA-2011-003.txt>
- Référence CVE CVE-2011-0284 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0284>

Gestion détaillée du document

16 mars 2011 version initiale.