

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans 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-2007-AVI-390>

Gestion du document

Référence	CERTA-2007-AVI-390
Titre	Vulnérabilités dans Kerberos
Date de la première version	06 septembre 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité du MIT MITKRB5-SA-2007-006.txt du 04 septembre 2007 Bulletin de sécurité Sun 103060 du 05 septembre 2007
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.

2 Systèmes affectés

Kerberos versions 5-1.4 à 5-1.6.2. La version 5-1.4 ainsi que la version déployée sur Sun Solaris ne sont pas concernées par la vulnérabilité référencée CVE-2007-4000.

3 Résumé

Deux vulnérabilités découvertes dans *Kerberos* 5 permettent l'exécution de code arbitraire à distance.

4 Description

Deux vulnérabilités ont été découvertes dans *Kerberos* 5 :

- un débordement de mémoire dans l'implémentation de `RPCSEC_GSS` permet l'exécution de code arbitraire à distance (référence CVE-2007-3999). D'autres applications utilisant la bibliothèque RPC fournie avec

Kerberos 5 peuvent être affectées ;

- le serveur d'administration de *Kerberos* (`kadmin`) peut écrire des données dans un pointeur non initialisé (référence CVE-2007-4000). Cette vulnérabilité est spécifique à l'implémentation MIT de *Kerberos*.

5 Solution

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

6 Documentation

- Bulletin de sécurité du MIT MITKRB5-SA-2007-006 du 04 septembre 2007 :
<http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2007-006.txt>
- Bulletin de sécurité Sun Solaris #103060 du 05 septembre 2007 :
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-103060-1>
- Référence CVE CVE-2007-3999 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3999>
- Référence CVE CVE-2007-4000 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4000>

Gestion détaillée du document

06 septembre 2007 version initiale.