Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 27 juillet 2007
N° CERTA-2007-AVI-284-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans MIT Kerberos 5

Gestion du document

Référence	CERTA-2007-AVI-284-001
Titre	Vulnérabilités dans MIT Kerberos 5
Date de la première version	28 juin 2007
Date de la dernière version	27 juillet 2007
Source(s)	Bulletin de sécurité du MIT MITKRB5-SA-2007-004 Bulletin de sécurité du MIT MITKRB5-SA-2007-005
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

MIT Kerberos 5 versions krb5-1.6.1 et antérieures.

3 Résumé

Plusieurs vulnérabilités affectant `MIT Kerberos 5` permettent à une personne d'exécuter du code arbitraire à distance.

4 Description

Trois vulnérabilités ont été identifiées dans le démon d'administration `kadmind` de `MIT Kerberos 5`. La première concerne un débordement de mémoire (CVE-2007-2798), les deux autres sont des erreurs au niveau de

la librairie `RPC` (CVE-2007-2442 et CVE-2007-2443). Ces vulnérabilités peuvent être exploitées par un attaquant pour exécuter du code arbitraire à distance.

Ces vulnérabilités ne concernent pas le protocole 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-2007-004 du 26 juin 2007 :
  http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2007-004.txt
- Bulletin de sécurité du MIT MITKRB5-SA-2007-00 du 26 juin 2007 :
  http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2007-005.txt
- Bulletin de sécurité SUN #102914 du 26 juin 2007 (CVE-2007-2442) :
  http://sunsolve.sun.com/search/docuement.do?assetkey=1-26-102914-1
- Bulletin de sécurité Gentoo GLSA-200707-11 du 25 juillet 2007 :
  http://www.gentoo.org/security/en/glsa/glsa-200707-11.xml
- Bulletin de sécurité Debian DSA-1323 du 28 juin 2007 :
  http://www.debian.org/security/2007/dsa-1323
- Bulletin de sécurité SuSE SUSE-SA:2007:038 du 03 juillet 2007 :
  http://www.novell.com/linux/security/advisories/2007_38_krb5.html
- Bulletin de sécurité Mandriva MDKSA-2007:137 du 26 juin 2007 :
  http://archives.mandrivalinux.com/security-announce/2007-06/msg00046.php
- Bulletin de sécurité Ubuntu USN-477-1 du 27 juin 2007 :
  http://www.ubuntu.com/usn/usn-477-1
- Bulletin de sécurité Red Hat RHSA-2007:0384-4 du 26 juin 2007 :
  http://rhn.redhat.com/errata/RHSA-2007-0384.html
- Bulletin de sécurité Red Hat RHSA-2007:0562-2 du 26 juin 2007 :
  http://rhn.redhat.com/errata/RHSA-2007-0562.html
- Référence CVE CVE-2007-2442 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2442
- Référence CVE CVE-2007-2443 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2443
- Référence CVE CVE-2007-2798 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2798

Gestion détaillée du document

28 juin 2007 version initiale.
27 juillet 2007 ajout des références aux bulletins de sécurité Gentoo, Debian et SuSE.