Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 25 juin 2010
N° CERTA-2010-AVI-219-002

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-219

Gestion du document

Référence	CERTA-2010-AVI-219-002
Titre	Vulnérabilité dans MIT Kerberos
Date de la première version	19 mai 2010
Date de la dernière version	25 juin 2010
Source	Bulletin de sécurité MITKRB5-SA-2010-005 du 18 mai 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

Déni de service à distance.

2 Systèmes affectés

MIT Kerberos versions krb5-1.8.1 et antérieures.

3 Résumé

Une vulnérabilité présente dans MIT Kerberos permet à un utilisateur distant authentifié de provoquer un déni de service.

4 Description

Une vulnérabilité de type pointeur nul est présente dans MIT Kerberos. Elle concerne potentiellement toutes les applications mettant en œuvre la bibliothèque de fonctions GSS-API. Cette faille permet à un utilisateur authentifié malintentionné de provoquer un déni de service à distance.

5 Solution

Se référer aux bulletins de sécurité des éditeurs pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Site de MIT Kerberos :
  http://web.mit.edu/kerberos
- Bulletin de sécurité MITKRB5-SA-2010-005 du 18 mai 2010 :
  http://web.mit.edu/kerberos/advisories/MITKRB5-SA-2010-005.txt
- Bulletin de sécurité Debian DSA-2052 du 24 mai 2010 :
  http://www.debian.org/security/2010/dsa-2052
- Bulletins de sécurité Fedora du 19 mai 2010 :
  http://lists.fedoraproject.org/pipermail/package-announce/2010-May/041615.html
  http://lists.fedoraproject.org/pipermail/package-announce/2010-May/041645.html
  http://lists.fedoraproject.org/pipermail/package-announce/2010-May/041654.html
- Bulletin de sécurité HP c02257427 du 23 juin 2010 :
  http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02257427
- Bulletin de sécurité Mandriva MDVSA-2010:100 du 19 mai 2010 :
  http://www.mandriva.com/security/advisories?name=MDVSA-2010:100
- Bulletin de sécurité RedHat RHSA-2010-0423-1 du 18 mai 2010 :
  http://rhn.redhat.com/errata/RHSA-2010-0423.html
- Bulletin de sécurité Suse SUSE-SR:2010:013 du 14 juin 2010 :
  http://lists.opensuse.org/opensuse-security-announce/2010-06/msg00001.html
- Bulletin de sécurité Ubuntu USN-940-1 du 19 mai 2010 :
  http://www.ubuntu.com/usn/usn-940-1
- Référence CVE CVE-2010-1321 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1321

Gestion détaillée du document

19 mai 2010 version initiale ;
25 mai 2010 ajout du bulletin de sécurité Debian.
25 juin 2010 ajout des bulletins de sécurité Fedora, HP, Mandriva, RedHat, Suse et Ubuntu.