Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 février 2005
N° CERTA-2004-AVI-411-004

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de MIT Kerberos 5

Gestion du document

Référence	CERTA-2004-AVI-411-004
Titre	Vulnérabilité de MIT Kerberos 5
Date de la première version	22 décembre 2004
Date de la dernière version	17 février 2005
Source(s)	Bulletin de sécurité MIT krb5 2004-004
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.

2 Systèmes affectés

MIT Kerberos 5 version krb5-1.3.5 et antérieures.

3 Description

Kerberos est un protocole d'authentification.

Une vulnérabilité de type débordement de mémoire est présente dans une routine de gestion de l'historique des mots-de-passe incluse dans la bibliothèque `libkadm5srv`.

Un utilisateur mal intentionné peut, après s'être préalablement authentifié, exploiter cette vulnérabilité pour exécuter du code arbitraire sur le serveur de clefs (KDC) vulnérable.

4 Solution

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

5 Documentation

- Bulletin de sécurité MIT krb5 2004-004 :
  http://web.mit.edu/kerberos/advisories/MITKRB5-SA-2004-004-pwhist.txt
- Bulletin de sécurité FreeBSD pour krb5 du 21 décembre 2004 :
  http://www.vuxml.org/freebsd/
- Bulletin de sécurité Mandrake MDKSA-2004:156 du 22 décembre 2004 :
  http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:156
- Bulletin de sécurité RedHat RHSA-2005-012 du 19 janvier 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-012.html
- Bulletin de sécurité RedHat RHSA-2005-045 du 15 février 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-045.html
- Bulletin de sécurité Gentoo GLSA 200501-05 du 05 janvier 2005 :
  http://www.gentoo.org/security/en/glsa/glsa-200501-05.xml
- Référence CVE CAN-2004-1189 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1189

Gestion détaillée du document

22 décembre 2004 version initiale.
23 décembre 2004 ajout référence au bulletin de sécurité Mandrake MDKSA-2004:156.
06 janvier 2005 ajout référence au bulletin de sécurité Gentoo GLSA 200501-05.
24 janvier 2005 ajout référence au bulletin de sécurité RedHat RHSA-2005-012.
17 février 2005 ajout référence au bulletin de sécurité RedHat RedHat RHSA-2005-045.