Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 septembre 2004
N° CERTA-2004-AVI-180-006

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de MIT Kerberos 5

Gestion du document

Référence	CERTA-2004-AVI-180-006
Titre	Vulnérabilité de MIT Kerberos 5
Date de la première version	04 juin 2004
Date de la dernière version	08 septembre 2004
Source(s)	Avis de sécurité de MIT krb5 2004-001
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 versions krb5-1.3.3 et antérieures.

3 Résumé

Plusieurs vulnérabilités de la fonction *krb5_aname_to_localname()* permettent à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

4 Description

Kerberos est un protocole d'authentification. La fonction *krb5_aname_to_localname()* de Kerberos permet de traduire un nom principal Kerberos en un nom de compte local (par exemple un utilisateur UNIX).
Plusieurs vulnérabilités de type débordement de mémoire permettent à un utilisateur distant mal intentionné d'exécuter du code arbitraire sur la machine vulnérable.

Seules les configurations qui utilisent des méthodes faisant appel à cette fonction sont vulnérables. Ce ne sont pas les configurations par défaut.

5 Solution

La version krb5-1.3.4 corrige ces vulnérabilités.
Il existe un correctif disponible sur le site de Kerberos (cf. section Documentation).
Consulter votre éditeur pour obtenir un éventuel correctif.

6 Documentation

- Bulletin de sécurité Kerberos 2004-001 :
  http://web.mit.edu/kerberos/advisories/MITKRB5-SA-2004-001-an_to_ln.txt
- Bulletin de sécurité VU#686862 de l'US-CERT :
  http://www.kb.cert.org/vuls/id/686862
- Bulletin de sécurité Mandrake MDKSA-2004:056 du 03 juin 2004 :
  http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:056
- Bulletin de sécurité RedHat RHSA-2004:236 du 09 juin 2004 :
  http://rhn.redhat.com/errata/RHSA-2004-236.html
- Bulletin de sécurité Debian DSA-520 du 16 juin 2004 :
  http://www.debian.org/security/2004/dsa-520
- Bulletin de sécurité Gentoo GLSA 200406-21 du 29 juin 2004 :
  http://www.gentoo.org/security/en/glsa/glsa-200406-21.xml
- Bulletin de sécurité #57580 de Sun :
  http://sunsolve.sun.com/search/document.do?assetkey=1-26-57580-1
- Mise à jour de sécurité du paquetage NetBSD mit-krb5 :
  ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/security/mit-krb5/README.html
- Bulletin de sécurité Apple du 07 septembre 2004 :
  http://docs.info.apple.com/article.html?artnum=61798
- Référence CVE CAN-2004-0523 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0523

Gestion détaillée du document

04 juin 2004 version initiale.

10 juin 2004 ajout de la référence au bulletin de sécurité de Red Hat.

14 juin 2004 ajout de la référence au bulletin de sécurité #57580 de Sun.

17 juin 2004 ajout de la référence au bulletin de sécurité Debian et de la référence CVE.

25 juin 2004 ajout de la référence au bulletin de sécurité NetBSD.

30 juin 2004 ajout de la référence au bulletin de sécurité Gentoo.

08 septembre 2004 ajout de la référence au bulletin de sécurité Apple et modification de la référence au bulletin de sécurité Sun.