Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 mai 2007
N° CERTA-2007-AVI-158-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de Kerberos

Gestion du document

Référence	CERTA-2007-AVI-158-001
Titre	Multiples vulnérabilités de Kerberos
Date de la première version	04 avril 2007
Date de la dernière version	30 mai 2007
Source(s)	Bulletin de sécurité Kerberos du 03 avril 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 ;
- déni de service à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

Kerberos 5.x.

Il n'est pas exclu que des produits tiers, utilisant *Kerberos*, soient affectés.

3 Résumé

Plusieurs vulnérabilités de *Kerberos* permettraient à des utilisateurs malveillants de provoquer un déni de service à distance, de contourner la politique de sécurité ou d'exécuter du code arbitraire à distance.

4 Description

Plusieurs vulnérabilités sont présentes dans *Kerberos* :

– une vulnérabilité du démon Telnet (`telnetd`) permet de se connecter avec un compte utilisateur quelconque. Si la configuration du démon exige l'authentification préalable, alors l'exploitation de cette vulnérabilité n'est possible que pour les utilisateurs authentifiés.

– une vulnérabilité dans l'utilisation de la fonction `krb5_klog_syslog()` permettrait à utilisateur malveillant authentifié d'exécuter du code arbitraire ou de provoquer un déni de service à distance. Les applications tierces utilisant cette fonction peuvent être vulnérables.

– une vulnérabilité du démon d'administration (`kadmind`) permettrait à un utilisateur authentifié d'exécuter du code arbitraire ou de provoquer un déni de service à distance. La source de la vulnérabilité est dans la bibliothèque de programmes GSS-API livrée avec *MIT krb5*. Par conséquent, les applications tierces utilisant cette bibliothèque peuvent être vulnérables.

5 Solution

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

6 Documentation

– Bulletin de sécurité Kerberos 2007-001 du 04 avril 2007 :
http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2007-001-telnetd.txt

– Bulletin de sécurité Kerberos 2007-002 du 04 avril 2007 :
http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2007-002-syslogd.txt

– Bulletin de sécurité Kerberos 2007-003 du 04 avril 2007 :
http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2007-003.txt

– Bulletin de sécurité HP #c01056923 du 15 mai 2007 :
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?lang=en&objectID=c01056923

– Bulletin de sécurité Gentoo GLSA-200704-02 du 03 avril 2007 :
http://www.gentoo.org/security/en/glsa/glsa-200704-02.xml

– Bulletin de sécurité Debian DSA-1276 du 03 avril 2007 :
http://www.debian.org/security/2007/dsa-1276

– Bulletin de sécurité Mandriva MDKSA-2007:077 du 04 avril 2007 :
http://www.mandriva.com/security/advisories?name=MDKSA-2007:077

– Bulletin de sécurité Red Hat RHSA-2007:0095 du 03 avril 2007 :
http://rhn.redhat.com/errata/RHSA-2007-0095.html

– Bulletin de sécurité Ubuntu USN-449-1 du 04 avril 2007 :
http://www.ubuntu.com/usn/usn-449-1

– Bulletin de sécurité SuSE SUSE-SA:2007:025 du 05 avril 2007 :
http://lists.suse.com/archive/suse-security-announce/2007-Apr/0001.html

– Référence CVE CVE-2007-0956 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0956

– Référence CVE CVE-2007-0957 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0957

– Référence CVE CVE-2007-1216 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1216

Gestion détaillée du document

04 avril 2007 version initiale.

30 mai 2007 ajout des références aux bulletins de sécurité HP, Gentoo, Debian, Mandriva, Red Hat, Ubuntu, SuSE.