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 mars 2008
N° CERTA-2008-AVI-154-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Kerberos

Gestion du document

Référence	CERTA-2008-AVI-154-001
Titre	Multiples vulnérabilités dans Kerberos
Date de la première version	20 mars 2008
Date de la dernière version	25 mars 2008
Source(s)	Bulletin de sécurité MITKRB5-SA-2008-001 du 18 mars 2008 Bulletin de sécurité MITKRB5-SA-2008-002 du 18 mars 2008
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 ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

Kerberos 5 versions 1.6.3 et antérieures.

3 Résumé

De multiples vulnérabilités dans *Kerberos 5* permettent de porter atteinte à la confidentialité des données, de réaliser un déni de service à distance et éventuellement, d'exécuter du code arbitraire à distance.

4 Description

Plusieurs vulnérabilités ont été découvertes dans *Kerberos 5* :

- l'utilisation d'un pointeur non initialisé pour certains types de messages `krb4` peut provoquer un déni de service ou l'exécution de code arbitraire à distance. L'exploitation de cette vulnérabilité nécessite l'activation du support *Kerberos 4*, ce qui n'est pas le cas par défaut (CVE-2008-0062) ;
- des messages `krb4` peuvent contenir des informations stockées en mémoire, ce qui peut porter atteinte à la confidentialité des données. L'exploitation de cette vulnérabilité nécessite l'activation du support *Kerberos 4* (CVE-2008-0063) ;
- un utilisateur malintentionné peut provoquer une corruption de la mémoire dans le processus `kadmind`, ce qui se traduit par un déni de service et, éventuellement, une exécution de code arbitraire à distance. L'exploitation de cette vulnérabilité nécessite des configurations qui permettent l'ouverture d'un grand nombre de descripteurs de fichier par processus (CVE-2008-0947 et CVE-2008-0948).

5 Solution

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

6 Documentation

- Bulletin de sécurité MITKRB5-SA-2008-001 du 18 mars 2008 :
  http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2008-001.txt
- Bulletin de sécurité MITKRB5-SA-2008-002 du 18 mars 2008 :
  http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2008-002.txt
- Bulletin de sécurité Gentoo GLSA-200803-31 du 24 mars 2008 :
  http://www.gentoo.org/security/en/glsa/glsa-200803-31.xml
- Bulletin de sécurité Debian DSA-1524 du 18 mars 2008 :
  http://www.debian.org/security/2008/dsa-1524
- Bulletin de sécurité Mandriva MDVSA-2008:069 du 19 mars 2008 :
  http://www.mandriva.com/en/security/advisroies?name=MDVSA-2008:069
- Bulletin de sécurité RedHat RHSA-2008:0180 du 18 mars 2008 :
  http://rhn.redhat.com/errata/RHSA-2008-0180.html
- Bulletin de sécurité Ubuntu USN-587-1 du 19 mars 2008 :
  http://www.ubuntulinux.org/usn/usn-587-1
- Référence CVE CVE-2008-0062 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0062
- Référence CVE CVE-2008-0063 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0063
- Référence CVE CVE-2008-0947 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0947
- Référence CVE CVE-2008-0948 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0948

Gestion détaillée du document

20 mars 2008 version initiale.

25 mars 2008 ajout des références aux bulletins de sécurité Gentoo, Debian et Mandriva.