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-286-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de MIT Kerberos 5

Gestion du document

Référence	CERTA-2004-AVI-286-003
Titre	Vulnérabilités de MIT Kerberos 5
Date de la première version	01 septembre 2004
Date de la dernière version	08 septembre 2004
Source(s)	Bulletins de sécurité MIT krb5 Security Advisory 2004-002 et 2004-003
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 ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

Toutes les versions de MIT Kerberos 5 antérieures à la version krb5-1.3.5.

3 Résumé

Plusieurs vulnérabilités dans MIT Kerberos 5 permettent à un utilisateur mal intentionné de réaliser un déni de service ou d'excécuter du code arbitraire à distance.

4 Description

MIT Kerberos est un protocole d'authentification.
Plusieurs vulnérabilités dans MIT Kerberos 5 ont été découvertes :

- Plusieurs vulnérabilités (CAN-2004-0642, CAN-2004-0643 et CAN-2004-0772) concernent des débordements de mémoire dans la mise en oeuvre du KDC (Key Distribution Center) ;

– plusieurs vulnérabilités (CAN-2004-0644) concernent des dénis de service dans le décodeur ASN.1 inclus dans MIT Kerberos 5.

Ces vulnérabilités permettent à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire à distance sur la plate-forme vulnérable.

5 Solution

Mettre à jour MIT Kerberos 5 en version krb5-1.3.5.
Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité MIT krb5 2004-002 :
  http://web.mit.edu/kerberos/advisories/MITKRB5-SA-2004-002-dblfree.txt
- Bulletin de sécurité MIT krb5 2004-003 :
  http://web.mit.edu/kerberos/advisories/MITKRB5-SA-2004-003-asn1.txt
- Bulletin de sécurité Debian DSA-543 du 31 août 2004 :
  http://www.debian.org/security/2004/dsa-543
- Bulletin de sécurité Mandrake MDKSA-2004:088 du 31 août 2004 :
  http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:088
- Bulletin de sécurité RedHat RHSA-2004:350 du 31 août 2004 :
  http://rhn.redhat.com/errata/RHSA-2004-350.html
- Bulletins de sécurité FreeBSD pour krb5 du 31 août 2004 :
  http://www.vuxml.org/freebsd/
- Bulletin de sécurité #57631 de Sun :
  http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/57631
- Bulletin de sécurité Cisco #61720 du 31 août 2004 :
  http://www.cisco.com/en/US/products/products_security_advisory09186a00802b3cf9.shtml
- Bulletin de sécurité Gentoo GLSA 200409-09 du 06 septembre 2004 :
  http://www.gentoo.org/security/en/glsa/glsa-200409-09.xml
- Mise à jour de sécurité du paquetage NetBSD mit-krb5 :
  ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/security/mit-krb5/README.html
- Référence CVE CAN-2004-0642 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0642
- Référence CVE CAN-2004-0643 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0643
- Référence CVE CAN-2004-0644 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0644
- Référence CVE CAN-2004-0772 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0772

Gestion détaillée du document

01 septembre 2004 version initiale.
02 septembre 2004 ajout de la référence au bulletin de sécurité Cisco.
06 septembre 2004 ajout de la référence au bulletin de sécurité Gentoo.
08 septembre 2004 ajout de la référence à la mise à jour de sécurité NetBSD.