

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans MIT Kerberos

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-595>

Gestion du document

Référence	CERTA-2011-AVI-595
Titre	Vulnérabilités dans MIT Kerberos
Date de la première version	26 octobre 2011
Date de la dernière version	–
Source	Bulletin de sécurité MIT Kerberos MITKRB5-SA-2011-006 du 22 octobre 2011
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 à distance.

2 Systèmes affectés

MIT Kerberos krb5-1.8 et krb5-1.9.

3 Résumé

Plusieurs vulnérabilités de MIT Kerberos permettent à un utilisateur non authentifié de provoquer un déni de service à distance.

4 Description

Dans MIT Kerberos, plusieurs vulnérabilités permettent à un utilisateur non authentifié de provoquer l'arrêt inopiné du serveur KDC.

L'une de ces vulnérabilités est générale. Les autres ne sont exploitables que si le KDC est adossé à un annuaire LDAP ou à une base de donnée Berkeley.

5 Solution

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

6 Documentation

- Bulletin de sécurité MIT Kerberos MITKRB5-SA-2011-006 du 22 octobre 2011 :
<http://web.mit.edu/kerberos/advisories/MITKRB5-SA-2011-006.txt>
- Bulletin de sécurité Mandriva MDVSA-2011:159 du 22 octobre 2011 :
<http://www.mandriva.com/fr/support/security/advisories?name=MDVSA-2011:159>
- Bulletin de sécurité Mandriva MDVSA-2011:160 du 22 octobre 2011 :
<http://www.mandriva.com/fr/support/security/advisories?name=MDVSA-2011:160>
- Bulletin de sécurité RedHat RHSA-2011:1379-1 du 18 octobre 2011 :
<http://rhn.redhat.com/errata/RHSA-2011-1379.html>
- Bulletin de sécurité Ubuntu USN-1233 du 18 octobre 2011 :
<http://www.ubuntu.com/usn/usn-1233-1/>
- Référence CVE CVE-2011-1527 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1527>
- Référence CVE CVE-2011-1528 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1528>
- Référence CVE CVE-2011-1529 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1529>
- Référence CVE CVE-2011-4151 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4151>

Gestion détaillée du document

26 octobre 2011 version initiale.