

FreeBSD-Security: krb5-1.3.2 is released (fwd)

krb5-1.3.2 is released (fwd)

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-02/0146.html>

From: Cy Schubert (Cy.Schubert_at_komquats.com)

Date: 02/27/04

To: FreeBSD-Security Mailing List <FreeBSD-Security@FreeBSD.org>, FreeBSD-Ports Mailing List <FreeBSD-Ports@FreeBSD.org>
Date: Thu, 26 Feb 2004 19:26:02 -0800

Just a quick heads up, I'm currently working on this. It's building on -CURRENT. Yet to be done, testing on -CURRENT, build & test on -STABLE, and verification of pkg-plist currency. I will post patches to the krb5 port to -security and -ports and assuming I don't get negative feedback, I will commit sometime late Saturday or on Sunday when I return from my trip Vancouver.

As crypto-publish.org does not yet distribute krb5-1.3.2, the crypto-publish.org section of the Makefile will continue to install krb5-1.3.1_3. This of course assumes pkg-plist compatibility. If changes need to be made to pkg-plist, crypto-publish.org fetch support will be temporarily disabled until they can post krb5-1.3.2 on their website.

Cheers,

--

Cy Schubert <Cy.Schubert@komquats.com> <http://www.komquats.com/>
BC Government . FreeBSD UNIX
Cy.Schubert@osg.gov.bc.ca . cy@FreeBSD.org
<http://www.gov.bc.ca/> . <http://www.FreeBSD.org/>

----- Forwarded Message

Date: Thu, 26 Feb 2004 20:15:12 -0500
From: Tom Yu <tlyu@MIT.EDU>
To: kerberos-announce@MIT.EDU
Subject: krb5-1.3.2 is released

- -----BEGIN PGP SIGNED MESSAGE-----

The MIT Kerberos Team announces the availability of MIT Kerberos 5 Release 1.3.2. Please see below for a list of some major changes since krb5-1.3.1, or consult the README file in the source tree for a more detailed list of significant changes.

RETRIEVING KERBEROS 5 RELEASE 1.3.2

=====

You may retrieve the Kerberos 5 Release 1.3.2 source from the following URL:

<http://web.mit.edu/kerberos/dist/>

The homepage for the krb5-1.3.2 release is:

<http://web.mit.edu/kerberos/krb5-1.3/>

Further information about Kerberos 5 may be found at the following URL:

<http://web.mit.edu/kerberos/>

MAJOR CHANGES SINCE RELEASE 1.3.1

=====

* Support for AES in GSSAPI has been implemented. This corresponds to

krb5-1.3.2 is released (fwd)

FreeBSD-Security: krb5-1.3.2 is released (fwd)

the in-progress work in the IETF (CFX).

- * Added a new ccache type "MSLSA:" for read-only access to the MS Windows LSA cache.
- * On Windows, krb5.exe now has a checkbox to request addressless tickets.
- * To avoid compatibility problems, unrecognized TGS options will now be ignored.
- * 128-bit AES has been added to the default enctypees.
- * AES cryptosystem now chains IVs. This WILL break backwards compatibility for the kcmd applications, if they are using AES session keys.

- -----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.0.7 (SunOS)

iQCVAwUBQD6aI6bDgE/zdoE9AQH+bwQAlC2pvr+DbnYNw8Nz1BAng6Hpqf3b5StJ
sZDakTpcOSalnouKv5TxRjLyG9hu9kz7e1Vl1/b9BDU5ROx9yTZnIV5PSxVO8JzR
QjfCM/hplk+UeEtc8lb63Thw//le4PBMc+8NM03Rmyiro4780SXKcbgyV+yF5ijD
Bj8AOFxdclA=
=uPfm

- -----END PGP SIGNATURE-----

kerberos-announce mailing list

kerberos-announce@mit.edu

<https://mailman.mit.edu/mailman/listinfo/kerberos-announce>

----- End of Forwarded Message

freebsd-security@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

To unsubscribe, send any mail to "freebsd-security-unsubscribe@freebsd.org"