Kerberos Security Advisories

MITKRB5-SA-2015-001
: Vulnerabilities in kadmind, libgssrpc, gss_process_context_token

MITKRB5-SA-2014-001
: Buffer overrun in kadmind with LDAP backend

MITKRB5-SA-2012-001
: KDC heap corruption and crash vulnerabilities

MITKRB5-SA-2011-008
: buffer overflow in telnet daemon and client

MITKRB5-SA-2011-007
: KDC null pointer dereference in TGS handling

MITKRB5-SA-2011-006
: KDC denial of service vulnerabilities

MITKRB5-SA-2011-005
: FTP daemon fails to set effective group ID

MITKRB5-SA-2011-004
: kadmind invalid pointer free()

MITKRB5-SA-2011-003
: KDC vulnerable to double-free when PKINIT enabled

MITKRB5-SA-2011-002
: KDC denial of service attacks

MITKRB5-SA-2011-001
: kpropd denial of service

MITKRB5-SA-2010-007
: Multiple checksum handling vulnerabilities

MITKRB5-SA-2010-006
: KDC uninitialized pointer crash in authorization data handling

MITKRB5-SA-2010-005
: GSS-API library null pointer dereference

MITKRB5-SA-2010-004
: double free in KDC

MITKRB5-SA-2010-003
: denial of service in kadmind in older krb5 releases

MITKRB5-SA-2010-002
: denial of service in SPNEGO

MITKRB5-SA-2010-001
: krb5-1.7 KDC denial of service

MITKRB5-SA-2009-004
: integer underflow in AES and RC4 decryption

MITKRB5-SA-2009-003
: KDC denial of service in cross-realm referral processing

MITKRB5-SA-2009-002
: ASN.1 decoder frees uninitialized pointer

MITKRB5-SA-2009-001
: multiple vulnerabilities in SPNEGO, ASN.1 decoder

MITKRB5-SA-2008-002
: array overrun in RPC library used by kadmind

MITKRB5-SA-2008-001
: double-free, uninitialized data vulnerabilities in krb5kdc

MITKRB5-SA-2007-006
: kadmind RPC library buffer overflow, uninitialized pointer

MITKRB5-SA-2007-005
: kadmind vulnerable to buffer overflow

MITKRB5-SA-2007-004
: kadmind affected by multiple RPC library vulnerabilities

MITKRB5-SA-2007-003
: double-free vulnerability in kadmind (via GSS-API library)

MITKRB5-SA-2007-002
: KDC, kadmind stack overflow in krb5_klog_syslog

MITKRB5-SA-2007-001
: telnetd allows login as arbitrary user

MITKRB5-SA-2006-003
: kadmind (via GSS-API mechglue) frees uninitialized pointers

MITKRB5-SA-2006-002
: kadmind (via RPC library) calls uninitialized function pointer

MITKRB5-SA-2006-001
: multiple local privilege escalation vulnerabilities

MITKRB5-SA-2005-003
: double-free in krb5_recvauth

MITKRB5-SA-2005-002
: buffer overflow, heap corruption in KDC

MITKRB5-SA-2005-001
: Buffer overflows in telnet client

MITKRB5-SA-2004-004
: Heap buffer overflow in libkadm5srv

MITKRB5-SA-2004-003
: ASN.1 decoder denial-of-service

MITKRB5-SA-2004-002
: Double-free vulnerabilities in KDC and libraries

MITKRB5-SA-2004-001
: Buffer overrun in aname_to_localname

MITKRB5-SA-2003-005:
: Buffer overrun and underrun in principal name handling

MITKRB5-SA-2003-004:
: Cryptographic weaknesses in Kerberos v4 protocol; KDC and realm compromise possible.

MITKRB5-SA-2003-003:
: Faulty length checks in xdrmem_getbytes may allow kadmind DoS.

MITKRB5-SA-2003-001:
: Multiple vulnerabilities, including possible KDC compromise, in older releases (prior to 1.2.5).

MITKRB5-SA-2002-002: [updated 2002-10-25] Buffer overflow in kadmind4
: Remote user can gain root access to KDC host.

MITKRB5-SA-2002-001: Remote root vulnerability in MIT krb5 admin system
: Remote user may be able to gain root access to a KDC host.

Buffer overflows in telnetd

Buffer overflows in ftpd

Unsafe temporary file handling in krb4 code
: A local user may overwrite arbitrary files as root

Remote root vulnerability in GSSFTPD
: An attacker with access to a local account may gain unauthorized root access via a krb5-1.1.x ftpd.

Multiple denial of service vulnerabilities in krb4 KDC
: A buffer overrun capable of causing a denial of service in the krb4 KDC compat code was discovered. Additionally, krb5-1.1.x KDCs with krb4 code enabled are vulnerable to a separate denial of service.

Buffer Overrun Vulnerabilities in Kerberos 4 code
: Serious buffer overruns exist in krb4 compatibility code. Also, these vulnerabilities likely exist in **almost all implementations** derived from MIT krb4.

Login bug when compiling using --without-krb4 in 1.1.1
: Compiling remote login programs using the --without-krb4 option has disastrous side effects under 1.1 and 1.1.1 releases.

MITKRB5-SA-2002-002-kadm4 attack signature

- Note describing attack signature associated with possible attacks on kadmind4.

Patches for MITKRB5-SA-2002-002-kadm4

- patch for krb5-1.2.6, with detached PGP signature

Patches for MITKRB5-SA-2002-001-xdr

- patch for krb5-1.2.5, with detached PGP signature

Patches for telnetd buffer overflow vulnerability

- Patch for krb5-1.2.2, with detached PGP signature

Patches for ftpd buffer overflow vulnerability

- Patch for krb5-1.2.2

Patches for krb4 temporary file vulnerability

- Patch for krb5-1.2.1

Patches for gssftpd vulnerability

- Patch for krb5-1.1.x ftpd

Patches for KDC vulnerabilities

- Patch for krb5-1.0.x KDCs
- Patch for krb5-1.1.1 KDC
- Patch for CNS KDC
- Untested patch for krb4 Patch 10

Patches for krb_rd_req() overruns:

The patches in some of the krb4 overrun original advisories have been untabified, which causes some people to have trouble applying them with the `patch` program. You may use "`patch -l`" if your version of patch supports it, or you may apply one of the patches below.

- Patch for krb4 buffer overruns in 1.0.x
- Patch for krb4 buffer overruns in 1.1.1 (includes patch for login.c)
- Patch for bug in login.c.

$Id: index.html,v 1.46 2016/07/01 17:34:45 ghudson Exp $
MIT Kerberos [home] [contact]