# CERT Advisory CA-1996-03 Vulnerability in Kerberos 4 Key Server

Original issue date: February 21, 1996
Last revised: September 24, 1997
Updated copyright statement

A complete revision history is at the end of this file.
The CERT Coordination Center has received reports of a vulnerability in the Kerberos Version 4 server. On unpatched Kerberos 4 systems, under certain circumstances, intruders can masquerade as authorized Kerberos users and gain access to services and resources not intended for their use. The CERT team recommends that you apply one of the solutions given in Section III.

The Kerberos Version 5 server running in Version 4 compatibility mode is also vulnerable under certain circumstances. The Massachusetts Institute of Technology (MIT) is working on the patches for that version.

We will update this advisory as we receive additional information. Please check advisory files regularly for updates that relate to your site.

---

## I. Description

The Kerberos Version 4 server is using a weak random number generator to produce session keys. On a computer of average speed, the session key for a ticket can be broken in a maximum of 2-4 minutes, and sometimes in much less time. This means that usable session keys can be manufactured without a user first being authorized by Kerberos.

## II. Impact

Under certain circumstances, intruders can masquerade as authorized Kerberos users and gain access to services and resources not intended for their use.

## III. Solution

If you are running Kerberos Version 4 and have built Kerberos from a source distribution, use solution A. If you have obtained Kerberos 4 binaries from a vendor, use solution B. If you are now using Kerberos Version 5, be aware that MIT is working on patches for that version. Notice will be made when the patches are available.

### A. Solution for Source Distributions

If you have built Kerberos Version 4 from source, follow these instructions to retrieve the fixes necessary to correct this problem:

> Use anonymous FTP to athena-dist.mit.edu. Change directory to /pub/kerberos, fetch and read "README.KRB4" found in that directory. It will provide the name of the distribution directory (which is otherwise hidden and cannot be found by listing its parent directory). Change directory to the hidden distribution directory. There you will find the original Kerberos distribution plus a new file named "random_patch.tar.Z" (and random_patch.tar.gz for those with "gzip"). This tar file contains two files, the patch itself and a README.PATCH file. Read this file carefully before proceeding.

As of February 23, 1996, MIT has updated the patch described in advisory CA-96.03. The actual patch has not changed, but the README.PATCH file (part of random_patch.tar.*) which contains instructions on how to install the patch has been edited to include the following new paragraph:

IMPORTANT: After running fix_kdb_keys you must kill and restart the kerberos server process (it has the old keys cached in memory). Also, if you operate any Kerberos slave servers, you need to perform a slave propagation immediately to update the keys on the slaves.

Updated files are now available on "athena-dist.mit.edu" including an updated random_patch.md5 file which contains the MD5 checksums of random_patch.tar.* The PGP Signature is issued by Jeffrey I. Schiller <jis@mit.edu> using PGP keyid 0x0DBF906D. The fingerprint is

DD DC 88 AA 92 DC DD D5 BA 0A 6B 59 C1 65 AD 01

The updated files are also available from

ftp://ftp.cert.org/pub/vendors/mit/Patches/Kerberos-V4/

The new checksums are

MD5 (random_patch.md5) = ecf5412094572e183aa33ae4e5f197b8
MD5 (random_patch.tar.Z) = e925b687a05a8c6321b2805026253315
MD5 (random_patch.tar.gz) = 003226914427094a642fd1f067f589d2

These files are also available from

ftp://ftp.cert.org/pub/vendors/mit/Patches/Kerberos-V4/random_patch.md5

ftp://ftp.cert.org/pub/vendors/mit/Patches/Kerberos-V4/random_patch.tar.Z

ftp://ftp.cert.org/pub/vendors/mit/Patches/Kerberos-V4/random_patch.tar.gz

The checksums are the same as above.

### B. Solution for Binary Distributions

Contact your vendor.
Some vendors who provide Kerberos are sending the CERT Coordination Center information about their patches. Thus far, we have received information from one vendor and placed it in the appendix of this advisory. We will update the appendix as we hear from vendors.

## Appendix A: Vendor Information

Below is information we have received from vendors concerning the vulnerability described in this advisory. If you do not see your vendor's name, please contact the vendor directly for information.

### The Santa Cruz Operation, Inc.

The Kerberos 4 problem does not affect SCO.

SCO OpenServer, SCO Open Desktop, SCO UnixWare, SCO Unix, and SCO Xenix do not support Kerberos.

The SCO Security Server, an add-on product for SCO OpenServer 3 and SCO OpenServer 5, supports Kerberos V5 authentication. This product cannot be configured to be Kerberos V4 compatible; therefore, it is not vulnerable.

### TGV Software, Inc.

TGV has made two Kerberos ECO kits available (one for MultiNet V3.4 and one for V3.5) for Anonymous FTP. If you are running Kerberos, we _strongly_ urge you to apply this kit.

To obtain the kit, FTP to ECO.TGV.COM, username ANONYMOUS, password either KERBEROS-034 or KERBEROS-035 (depending on the version of MultiNet that you are running) and download the ECO kit:

ftp://anonymous:kerberos-035@eco.tgv.com

The kit is available in both VMS BACKUP save set format as well as in a compressed .ZIP file. Use VMSINSTAL to apply the ECO.

Once you have completed the upgrade, the KITREMARK.VUR file from the ECO kit will be displayed providing instructions during the installation process.

If you have any questions, please send an e-mail message to

MultiNet-VMS@Support.TGV.COM

### Transarc Corporation

Kerberos Version 4.0 is used in our AFS product (all versions of AFS), while Kerberos Version 5.0 is used in our DCE product (Kerberos Version 5.0 is used in ALL DCE products).

In light of the COAST work, Transarc is doing a security review of Kerberos 4.0 and AFS. We expect to provide some procedural changes to improve security in new cells, and we will make code changes as necessary. OSF also reviewed Kerberos 5.0, and they have released a source patch for Kerberos 5.0 that strengthens the random number generator in Kerberos 5.0. This patch is relevant to all versions of DCE (but not to AFS since it is based on Kerberos 4.0).

Transarc has this OSF patch available for DCE 1.1 on Solaris 2.4, DCE 1.0.3a on Solaris 2.4, DCE 1.0.3a on Solaris 2.3, and DCE 1.0.3a on Sun OS 4.1.3. Please contact Transarc Customer Support for access to these patches.

Please feel free to contact me directly if you have further questions about this issue.

For pointers and background on these issues please refer to
http://www.transarc.com/afs/transarc.com/public/www/Public/Support/security-\ update.html

Liz Hines
Hines@transarc.com

The CERT Coordination Center thanks Jeffrey Schiller and Theodore Ts'o of Massachusetts Institute of Technology for their effort in responding to this problem, and thanks Gene Spafford of COAST for the initial information about the problem.

Revision History

```
Sep. 24, 1997 Updated copyright statement
Aug. 30, 1996 Information previously in the README was inserted into
              the advisory.
Mar. 08, 1996 Appendix, TGV Software & Transarc - added entries
Feb. 23, 1996 Sec. III.A - noted a change in the readme.patch file and
              put new MD5 checksums at the end of the section.
```