Keeping FreeBSD Up-To-Date

Richard Bejtlich (taosecurity at gmail dot com)

25 August 2009

Sections:

Introduction

An important system administration task, and a principle of running a defensible network, is keeping operating systems and applications up-to-date. Running current software is critical when older services are vulnerable to exploitation. Obtaining new features not found in older applications is another reason to run current software. Fortunately, open source software offers a variety of means to give users a secure, capable computing environment.

This article presents multiple ways to keep the FreeBSD operating system up-to-date. I take a FreeBSD 7.1 RELEASE system through a subset of security advisories to explain the different sorts of patches an administrator might apply. It is important to realize that this article discusses the OS only; it does not discuss applications. FreeBSD does not have a unified update mechanism for the OS and applications. By applications I mean software outside of the kernel and userland. For example, Debian systems can use the apt tool to keep the distribution and packaged applications up-to-date. FreeBSD does not have a single equivalent tool, so this article only addresses keeping the OS up-to-date.

Note that there is a difference between an update and an upgrade. I use the term update to refer to keeping a certain version of FreeBSD up-to-date. For example, keeping a FreeBSD 7.1 system at version 7.1, but having the appropriate security and critical patches applied, qualifies an update process. I use the term upgrade to refer to changing the FreeBSD version, either within a minor version or to a new major version. For example, migrating from FreeBSD 7.1 to 7.2, or from 7.2 to 8.0, qualify as upgrade processes.

I chose FreeBSD 7.1, released in January 2009, as my starting point because it offers a security history suitable for describing multiple update cases. At the time of writing FreeBSD 7.2 is the latest STABLE release and 8.0 is in BETA. Readers wondering why someone might want to install an "old" OS version can imagine that there might be an application supported only on FreeBSD 7.1 and not yet officially ready for 7.2 or 8.0, prompting an administrator to run a 7.1 box.

All of the work done in this article was done remotely via OpenSSH. One danger of performing remote upgrades is losing connection during a critical phase of the process. One software-based way to deal with this issue is to conduct all remote upgrades within a screen(1) session. (http://www.freshports.org/misc/screen) Should you lose connectivity during the upgrade while running screen, your session will continue uninterrupted. The screen(1) program has suffered security problems in the past, so balance its features against the possible risks.

My advice on administering this reference platform is based on deploying FreeBSD on servers, workstations, and laptops since 2000. The article represents a mix of my interpretations of official FreeBSD documentation, inputs from mentors, and the result of my own experimentation and deployment strategies. This guide cannot be anywhere near a complete reference on keeping FreeBSD up-to-date or maintaining a secure system. I strongly recommend reading the excellent FreeBSD Handbook as well as the multiple helpful published books on FreeBSD.

FreeBSD Handbook and Absolute FreeBSD, 2nd Ed

Please note that Chapter 24, Updating and Upgrading FreeBSD, is the authoritative source for information on keeping the FreeBSD OS up-to-date (http://www.freebsd.org/doc/en/books/handbook/updating-upgrading.html). The reason I wrote this article was to show how these various mechanisms apply in practice, and which I prefer in production.

I must also recommend Michael W. Lucas' excellent book Absolute FreeBSD, 2nd Ed (No Starch, 2008). Several other excellent FreeBSD writers have produced books, but Michael's is my favorite. For deeper coverage on the topics in this article, please see the Handbook or Michael's book.

The Short Answer: Updating FreeBSD with Binary Upgrades

If you want to jump straight to the easiest way to keep the FreeBSD OS up-to-date, without changing major or minor versions, and you are a standard user who has not customized his or her kernel and userland, follow these instructions. I present this first and with little introduction because it is the most basic and important step for keeping the FreeBSD OS up-to-date for the majority of users.

1. Set proxy, if necessary using 'setenv HTTP_PROXY http://myproxy:myport'.
2. Run 'freebsd-update fetch'.
3. Run 'freebsd-update install'.
4. Reboot.

These steps are demonstrated on a FreeBSD 7.2 system installed from CD.

```
freebsd7a# uname -a
FreeBSD freebsd7a.localdomain 7.2-RELEASE FreeBSD 7.2-RELEASE #0: Fri May  1 08:49:13 UTC 2009
root@walker.cse.buffalo.edu:/usr/obj/usr/src/sys/GENERIC  i386

freebsd7a# setenv HTTP_PROXY http://172.16.2.1:3128

Looking up update.FreeBSD.org mirrors... 3 mirrors found.
Fetching public key from update5.FreeBSD.org... done.
Fetching metadata signature for 7.2-RELEASE from update5.FreeBSD.org... done.
Fetching metadata index... done.
Fetching 2 metadata files... done.
Inspecting system... done.
Preparing to download files... done.
Fetching 26 patches.....10....20... done.
Applying patches... done.

The following files will be updated as part of updating to 7.2-RELEASE-p3:
/boot/kernel/if_bce.ko
/boot/kernel/if_bce.ko.symbols
/boot/kernel/if_fxp.ko
/boot/kernel/if_fxp.ko.symbols
/boot/kernel/kernel
/boot/kernel/kernel.symbols
/lib/libc.so.7
/lib/libthr.so.3
...edited...
/usr/sbin/named
/usr/sbin/nologin
/usr/sbin/ntpd

freebsd7a# freebsd-update install
Installing updates... done.
```

```
freebsd7a# reboot

freebsd7a# uname -a
FreeBSD freebsd7a.localdomain 7.2-RELEASE-p2 FreeBSD 7.2-RELEASE-p2 #0: Wed Jun 24 00:57:44 UTC 2009
root@i386-builder.daemonology.net:/usr/obj/usr/src/sys/GENERIC  i386
```

Following those six steps will keep a generic FreeBSD system up-to-date.

Colin Percival's FreeBSD Update tool is one of the best new aspects of FreeBSD, in my opinion. Prior to applying binary updates, FreeBSD administrators had to rely on recompiling source code whenever updates needed to be applied. This included casual users operating standard systems as well as power users operating custom systems. With FreeBSD Update, casual users who are not making changes to the standard kernel and userland can quickly and easily keep the FreeBSD OS up-to-date. With some careful use, even power users can benefit from binary updates.

The rest of the article demonstrates additional methods and details, depending on the administrator's needs.

Understanding FreeBSD Versions

Before explaining ways to keep the FreeBSD OS up-to-date, I must briefly expand on the idea of the term "up-to-date." Thanks to FreeBSD's open source development methodology, any version of FreeBSD is available via check out from the Concurrent Versions System (CVS). (http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/anoncvs.html) These versions can be represented by CVS revision tags. (http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/cvs-tags.html) The following examples begin with 7.2 RELEASE, the most recently published version of FreeBSD:

- RELENG_7_2_0_RELEASE is FreeBSD 7.2 RELEASE, just as you might get on CD. RELENG_7_2_0_RELEASE is also known as a "release tag."
- RELENG_7_2 is the "security" branch for 7.2, which is FreeBSD 7.2 RELEASE with patches for security advisories and critical fixes applied. RELENG_7_2 is known as a "branch tag."
- RELENG_7 is the development line of the FreeBSD 7 tree, also known as 7-STABLE. RELENG_7 is also a "branch tag."
- . ("dot"), also known as HEAD, is the development line of the next version of FreeBSD, 8.0, also known as 8-CURRENT or simply CURRENT.

Linux users should note that these CVS revision tags do not pertain to the FreeBSD kernel alone. FreeBSD is developed as an integrated system, with a kernel matching userland tools. One should not run a kernel compiled for FreeBSD 7.2 RELEASE on a CURRENT machine. The kernel and all userland utilities are meant to be upgraded simultaneously, and must be kept synchronized. While Linux users are usually forced to acknowledge this good system administration practice when they upgrade major versions of their kernel (e.g., 2.4 to 2.6), they often maintain the same userland across minor kernel versions. FreeBSD strongly encourages users to always keep the userland and kernel in sync using the methods explained in the Handbook and elaborated upon in this document.

When thinking of what it means to be "up-to-date," one can see that the "oldest" version of FreeBSD as of version 7.2 is that which was most recently "pressed to CD" -- RELENG_7_2_0_RELEASE or FreeBSD 7.2 RELEASE. The "newest" would be HEAD or CURRENT, a constantly moving target modified and improved on a daily basis. How does an administrator decide what to run on her machines?

I prefer to begin a system's life by installing RELEASE software, like FreeBSD 7.2 RELEASE. As long as the systems performs as I would expect it to, I then track the RELENG_7_2 or "security" branch. This allows me to incorporate critical bug and security fixes that could jeopardize the system.

Occasionally I may encounter a system that requires a feature (like supporting a new piece of hardware) not present in the RELEASE or security branches. In cases where that feature is supported by STABLE, I will upgrade to that branch. In the rare cases where not even STABLE has the feature I need, I might install a snapshot of the CURRENT branch. I do not recommend running CURRENT in production environments as it is not supported like the RELEASE or STABLE versions are.

Learning About Security Issues

FreeBSD security advisories are published at the FreeBSD security page and at the freebsd-security-notifications mailing list. (http://www.freebsd.org/security/advisories.html and http://lists.freebsd.org/pipermail/freebsd-security-notifications/) I recommend all FreeBSD users subscribe to the moderated, very low volume notification mailing list. The advisories provide background, a problem description, an impact statement, workaround advice, a solution to fix the problem, and correction details. We'll take a closer look at an actual security advisory when we learn how to apply patches manually to the operating system.

Starting with the Installation

Let's start with the most common deployment scenario, using FreeBSD 7.1 RELEASE as our starting point. For this version, the CVS tag is RELENG_7_1_0_RELEASE for the version shipped on CD and RELENG_7_1 for the security branch.

The administrator installs FreeBSD 7.1 RELEASE from CD on a new server. She installs the User distribution set ("Average User -- binaries and doc only) and installs the ports tree. When installation is done, a check of uname output shows what the system looks like prior to any changes:

```
freebsd7# uname -a
FreeBSD freebsd7.localdomain 7.1-RELEASE FreeBSD 7.1-RELEASE #0: Thu Jan  1 14:37:25 UTC 2009
root@logan.cse.buffalo.edu:/usr/obj/usr/src/sys/GENERIC  i386
```

She does not need to modify the kernel and is running the GENERIC version shipped with the OS.

At this point the system is running, but it requires security updates.

Installing Gnupg and Importing Keys

Whenever an administrator wants to manually apply a security patch, it is important to validate those patches using Gnu Privacy Guard (Gnupg, http://www.freshports.org/security/gnupg). In this section we will install Gnupg and import FreeBSD developer keys.

```
freebsd7# pkg_add -vr gnupg
scheme:   [ftp]
user:     []
password: []
host:     [ftp.freebsd.org]
port:     [0]
document: [/pub/FreeBSD/ports/i386/packages-7.1-release/Latest/gnupg.tbz]
---> ftp.freebsd.org:21
looking up ftp.freebsd.org
connecting to ftp.freebsd.org:21
<<< 220 Welcome to freebsd.isc.org.
>>> USER anonymous
<<< 331 Please specify the password.
>>> PASS analyst@freebsd7.localdomain
<<< 230 Login successful.
>>> PWD
<<< 257 "/"
>>> CWD pub/FreeBSD/ports/i386/packages-7.1-release/Latest
<<< 250 Directory successfully changed.
>>> MODE S
<<< 200 Mode set to S.
>>> TYPE I
<<< 200 Switching to Binary mode.
setting passive mode
>>> PASV
<<< 227 Entering Passive Mode (204,152,184,73,174,202)
opening data connection
initiating transfer
>>> RETR gnupg.tbz
<<< 150 Opening BINARY mode data connection for gnupg.tbz (929353 bytes).
Fetching ftp://ftp.freebsd.org/pub/FreeBSD/ports/i386/packages-7.1-release/Latest/gnupg.tbz...x +CONTENTS
x +COMMENT
x +DESC
x +INSTALL
x +DISPLAY
x +MTREE_DIRS
x man/man1/gpg2.1.gz
```

```
x man/man1/gpgsm.1.gz
x man/man1/gpgv2.1.gz
...edited...
Package gnupg-2.0.9_2 registered in /var/db/pkg/gnupg-2.0.9_2
...truncated...
```

Notice in the output above that the version of Gnupg shipped with FreeBSD 7.1 (in packages-7.1-release) is the version installed automatically here.

Next we import required PGP keys.

```
freebsd7# gpg --import /usr/share/doc/en_US.ISO8859-1/books/handbook/pgpkeys.html
gpg: directory `/root/.gnupg' created
gpg: new configuration file `/root/.gnupg/gpg.conf' created
gpg: WARNING: options in `/root/.gnupg/gpg.conf' are not yet active during this run
gpg: keyring `/root/.gnupg/secring.gpg' created
gpg: keyring `/root/.gnupg/pubring.gpg' created
gpg: /root/.gnupg/trustdb.gpg: trustdb created
gpg: key CA6CDFB2: public key "FreeBSD Security Officer <security-officer@FreeBSD.org>" imported
gpg: key FF8AE305: public key "core-secretary@FreeBSD.org" imported
gpg: key 7414629C: public key "FreeBSD portmgr secretary <portmgr-secretary@FreeBSD.org>" imported
gpg: Total number processed: 3
gpg:               imported: 3  (RSA: 1)
gpg: no ultimately trusted keys found
```

With Gnupg installed, you will be able to check signatures on patches applied later.

Installing Source Code

When the administrator installed FreeBSD 7.1, she did not install the source code for the system. We'll do that next.

FreeBSD source code can either be checked out from CVS online, or installed from other media. Since this system was just installed from CD, and we have the CD handy, we'll install the source code from CD.

The easiest way to install source code from CD is to use the sysinstall program.

First, note that the source code is not available yet on the system.

```
freebsd7# ls /usr/src
freebsd7#
```

Launch 'sysinstall'.

1. Select 'Configure - Do post-install configuration of FreeBSD'
2. Select 'Distributions - Install additional distribution sets'
3. Select 'src - Sources for everything' by highlighting and hitting the space bar
4. Select 'All - Select all of the below' by highlighting and hitting return. Tab to OK and hit return.
5. Tab to OK on the 'Select the distributions you wish to install' page and hit return.
6. Select 'CD/DVD - Install from a FreeBSD CD/DVD' and hit return.
7. Wait until the source code is installed, then exit sysinstall.

Now, listing /usr/src shows the source code is installed.

```
freebsd7# ls /usr/src
COPYRIGHT               contrib                 rescue
LOCKS                   crypto                  sbin
MAINTAINERS             etc                     secure
Makefile                games                   share
Makefile.inc1           gnu                     sys
ObsoleteFiles.inc       include                 tools
README                  kerberos5               usr.bin
UPDATING                lib                     usr.sbin
bin                     libexec
cddl                    release
```

An alternative to installing the source code from CD involves using cvs to check it out. In this example we access an anonynous FreeBSD CVS server (http://www.freebsd.org/doc/en/books/handbook/anoncvs.html). For example:

```
freebsd7# cd /usr

freebsd7# cvs -d anoncvs@anoncvs1.freebsd.org:/home/ncvs co -r RELENG_7_0_0 src
cvs checkout: Updating src
cvs checkout: Updating src/bin
cvs checkout: Updating src/bin/cat
...truncated...
```

With the source code on the system, you will be able to manually apply patches and recompile the whole system or kernel as necessary.

Installing CVSup

The final addition to our FreeBSD 7.1 RELEASE system is the cvsup-without-gui package.

```
freebsd7# pkg_add -vr cvsup-without-gui
...edited...
x bin/cvpasswd
x bin/cvsup
x sbin/cvsupd
...edited...
Package cvsup-without-gui-16.1h_4 registered in /var/db/pkg/cvsup-without-gui-16.1h_4
```

It turns out that CVSup isn't really needed on modern FreeBSD systems, but I include it here because it is the single most recognizable update tool for FreeBSD.

At this point we have the infrastructure in place to try applying patches as required.

Applying Kernel Patches Manually

In the following sections we will examine a variety of ways to keep FreeBSD up-to-date. In this section we will look at applying kernel patches manually. We've already seen how FreeBSD can make updating the GENERIC kernel very easy. However, the situation becomes more complicated when administrators run custom kernels or make other local modifications.

To demonstrate how to manually patch the FreeBSD kernel on our FreeBSD 7.1 RELEASE system, we will use the FreeBSD-SA-09:06.ktimer advisory as an example (http://security.freebsd.org/advisories/FreeBSD-SA-09:06.ktimer.asc).

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

=============================================================================
FreeBSD-SA-09:06.ktimer                                     Security Advisory
                                                          The FreeBSD Project

Topic:          Local privilege escalation

Category:       core
Module:         kern
Announced:      2009-03-23
Affects:        FreeBSD 7.x
Corrected:      2009-03-23 00:00:50 UTC (RELENG_7, 7.2-PRERELEASE)
                2009-03-23 00:00:50 UTC (RELENG_7_1, 7.1-RELEASE-p4)
                2009-03-23 00:00:50 UTC (RELENG_7_0, 7.0-RELEASE-p11)
CVE Name:       CVE-2009-1041

For general information regarding FreeBSD Security Advisories,
including descriptions of the fields above, security branches, and the
following sections, please visit <URL:http://security.FreeBSD.org/>.
```

I.   Background

In FreeBSD 7.0, support was introduced for per-process timers as defined in the POSIX realtime extensions. This allows a process to have a limited number of timers running at once, with various actions taken when each timer reaches zero.

II. Problem Description

An integer which specifies which timer a process wishes to operate upon is not properly bounds-checked.

III. Impact

An unprivileged process can overwrite an arbitrary location in kernel memory. This could be used to change the user ID of the process (in order to "become root"), to escape from a jail, or to bypass security mechanisms in other ways.

IV. Workaround

No workaround is available, but systems without untrusted local users are not vulnerable.

V.   Solution

Perform one of the following:

1) Upgrade your vulnerable system to 7-STABLE, or to the RELENG_7_1 or RELENG_7_0 security branch dated after the correction date.

2) To patch your present system:

The following patch has been verified to apply to FreeBSD 7.0 and 7.1 systems.

a) Download the relevant patch from the location below, and verify the detached PGP signature using your PGP utility.

```
# fetch http://security.FreeBSD.org/patches/SA-09:06/ktimer.patch
# fetch http://security.FreeBSD.org/patches/SA-09:06/ktimer.patch.asc
```

b) Apply the patch.

```
# cd /usr/src
# patch < /path/to/patch
```

c) Recompile your kernel as described in <URL:http://www.FreeBSD.org/handbook/kernelconfig.html> and reboot the system.

VI. Correction details

The following list contains the revision numbers of each file that was corrected in FreeBSD.

CVS:

Branch Path	Revision
RELENG_7	
src/sys/kern/kern_time.c	1.142.2.3
RELENG_7_1	
src/UPDATING	1.507.2.13.2.7
src/sys/conf/newvers.sh	1.72.2.9.2.8
src/sys/kern/kern_time.c	1.142.2.2.2.2

```
RELENG_7_0
  src/UPDATING                                             1.507.2.3.2.15
  src/sys/conf/newvers.sh                                   1.72.2.5.2.15
  src/sys/kern/kern_time.c                                      1.142.4.1
- -------------------------------------------------------------------------

Subversion:

Branch/path                                                      Revision
- -------------------------------------------------------------------------
stable/7/                                                         r190301
releng/7.1/                                                       r190301
releng/7.0/                                                       r190301
- -------------------------------------------------------------------------

VII. References

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1041

The latest revision of this advisory is available at
http://security.FreeBSD.org/advisories/FreeBSD-SA-06:09.ktimer.asc
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.9 (FreeBSD)

iEYEARECAAYFAknG0hQACgkQFdaIBMps37JA4gCfaznvIWKB/AU0cv6ojZUhheD4
MuYAnAp3wuz3E7gIX6VK7PeUVnPp/41o
=MPIX
-----END PGP SIGNATURE-----
```

To implement this advisory, we follow the instructions in part 2.

```
freebsd7# fetch http://security.FreeBSD.org/patches/SA-09:06/ktimer.patch
ktimer.patch                                  100% of  476  B   61 kBps

freebsd7# fetch http://security.FreeBSD.org/patches/SA-09:06/ktimer.patch.asc
ktimer.patch.asc                              100% of  195  B   24 kBps
```

Next we validate the patch.

```
freebsd7# gpg --verify ktimer.patch.asc ktimer.patch
gpg: Signature made Sun Mar 22 19:59:58 2009 EDT using DSA key ID CA6CDFB2
gpg: Good signature from "FreeBSD Security Officer <security-officer@FreeBSD.org>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: C374 0FC5 69A6 FBB1 4AED  B131 15D6 8804 CA6C DFB2
```

GPG warns us that we have not taken any steps to trust the signature of the FreeBSD Security Officer. One of the ways to make this warning disappear would be to sign the key of the FreeBSD Security Officer ourselves. We might do that after confirming in person or on the telephone that the primary key fingerprint of the FreeBSD Security Officer's key is as stated in the output above. (Beyond this example, I will not show verifying future patches.)

For now we assume that the patch has not been tampered with and move on to applying it per the advisory's instructions:

Now we apply the patch.

```
freebsd7# patch < /root/ktimer.patch
Hmm...  Looks like a unified diff to me...
The text leading up to this was:
--------------------------
|Index: sys/kern/kern_time.c
|===================================================================
|--- sys/kern/kern_time.c       (revision 190192)
|+++ sys/kern/kern_time.c       (working copy)
--------------------------
Patching file sys/kern/kern_time.c using Plan A...
```

```
Hunk #1 succeeded at 1079 (offset -6 lines).
done
```

Finally we compile a new kernel for our system. Note that we decide to make a copy of the configuration file called FREEBSD7. We do not leave the kernel as GENERIC because we have patched it.

```
freebsd7# cd /usr/src/sys/i386/conf
freebsd7# cp GENERIC FREEBSD7
freebsd7# cd /usr/src
freebsd7# make buildkernel KERNCONF=FREEBSD7

--------------------------------------------------------------
>>> Kernel build for FREEBSD7 started on Thu Aug 20 11:01:55 EDT 2009
--------------------------------------------------------------
===> FREEBSD7
mkdir -p /usr/obj/usr/src/sys

--------------------------------------------------------------
>>> stage 1: configuring the kernel
--------------------------------------------------------------
cd /usr/src/sys/i386/conf;  PATH=/usr/obj/usr/src/tmp/legacy/usr/sbin:/usr/obj/usr/src/tmp/legacy/usr/
bin:/usr/obj/usr/src/tmp/legacy/usr/games:/usr/obj/usr/src/tmp/usr/sbin:/usr/obj/usr/src/tmp/usr/bin:/usr/
obj/usr/src/tmp/usr/games:/sbin:/bin:/usr/sbin:/usr/bin  config  -d /usr/obj/usr/src/sys/FREEBSD7  /usr/
src/sys/i386/conf/FREEBSD7
Kernel build directory is /usr/obj/usr/src/sys/FREEBSD7
...edited...
--------------------------------------------------------------
>>> Kernel build for FREEBSD7 completed on Thu Aug 20 11:54:29 EDT 2009
--------------------------------------------------------------
```

After waiting several minutes we install the new kernel.

```
freebsd7# make installkernel KERNCONF=FREEBSD7
--------------------------------------------------------------
>>> Installing kernel
--------------------------------------------------------------
cd /usr/obj/usr/src/sys/FREEBSD7;  MAKEOBJDIRPREFIX=/usr/obj  MACHINE_ARCH=i386  MACHINE=i386  CPUTYPE=
GROFF_BIN_PATH=/usr/obj/usr/src/tmp/legacy/usr/bin  GROFF_FONT_PATH=/usr/obj/usr/src/tmp/legacy/usr/share/
groff_font  GROFF_TMAC_PATH=/usr/obj/usr/src/tmp/legacy/usr/share/tmac PATH=/usr/obj/usr/src/tmp/legacy/
usr/sbin:/usr/obj/usr/src/tmp/legacy/usr/bin:/usr/obj/usr/src/tmp/legacy/usr/games:/usr/obj/usr/src/tmp/
usr/sbin:/usr/obj/usr/src/tmp/usr/bin:/usr/obj/usr/src/tmp/usr/games:/sbin:/bin:/usr/sbin:/usr/bin  make
KERNEL=kernel install
thiskernel=`sysctl -n kern.bootfile` ;  if [ ! "`dirname "$thiskernel"`" -ef /boot/kernel ] ; then
chflags -R noschg /boot/kernel ;  rm -rf /boot/kernel ;  else  if [ -d /boot/kernel.old ] ; then  chflags
-R noschg /boot/kernel.old ;  rm -rf /boot/kernel.old ;  fi ;  mv /boot/kernel /boot/kernel.old ;  sysctl
kern.bootfile=/boot/kernel.old/"`basename "$thiskernel"`" ;  fi
kern.bootfile: /boot/kernel/kernel -> /boot/kernel.old/kernel
mkdir -p /boot/kernel
install -p -m 555 -o root -g wheel kernel /boot/kernel
...edited...
install -o root -g wheel -m 555   if_zyd.ko.symbols /boot/kernel
kldxref /boot/kernel
```

After a final check of the installed kernel (which is still running), we reboot.

```
freebsd7# uname -a
FreeBSD freebsd7.localdomain 7.1-RELEASE FreeBSD 7.1-RELEASE #0: Thu Jan  1 14:37:25 UTC 2009
root@logan.cse.buffalo.edu:/usr/obj/usr/src/sys/GENERIC  i386
freebsd7# reboot
```

After reboot, notice that the new kernel is installed.

```
freebsd7# uname -a
FreeBSD freebsd7.localdomain 7.1-RELEASE FreeBSD 7.1-RELEASE #0: Thu Aug 20 11:24:04 EDT 2009
root@freebsd7.localdomain:/usr/obj/usr/src/sys/FREEBSD7  i386
```

The compilation date also matches the date the new kernel was compiled.

Applying Userland Patches Manually

In the previous section we saw how to apply a patch to the kernel, then recompile and install the patched kernel. Here we will look at applying a patch to a userland application that ships with the FreeBSD OS. For this example we will use the FreeBSD-SA-09:05.telnetd advisory (http://security.freebsd.org/advisories/FreeBSD-SA-09:05.telnetd.asc).

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

=============================================================================
FreeBSD-SA-09:05.telnetd                                    Security Advisory
                                                          The FreeBSD Project

Topic:          telnetd code execution vulnerability

Category:       core
Module:         contrib
Announced:      2009-02-16
Affects:        FreeBSD 7.x
Corrected:      2009-02-16 21:56:17 UTC (RELENG_7, 7.1-STABLE)
                2009-02-16 21:56:17 UTC (RELENG_7_1, 7.1-RELEASE-p3)
                2009-02-16 21:56:17 UTC (RELENG_7_0, 7.0-RELEASE-p10)

For general information regarding FreeBSD Security Advisories,
including descriptions of the fields above, security branches, and the
following sections, please visit <URL:http://security.FreeBSD.org/>.

I.   Background

The FreeBSD telnet daemon, telnetd(8), implements the server side of the
TELNET virtual terminal protocol.  It has been disabled by default in
FreeBSD since August 2001, and due to the lack of cryptographic security
in the TELNET protocol, it is strongly recommended that the SSH protocol
be used instead.  The FreeBSD telnet daemon can be enabled via the
/etc/inetd.conf configuration file and the inetd(8) daemon.

The TELNET protocol allows a connecting client to specify environment
variables which should be set in any created login session; this is used,
for example, to specify terminal settings.

II.  Problem Description

In order to prevent environment variable based attacks, telnetd(8) "scrubs"
its environment; however, recent changes in FreeBSD's environment-handling
code rendered telnetd's scrubbing inoperative, thereby allowing potentially
harmful environment variables to be set.

III. Impact

An attacker who can place a specially-constructed file onto a target system
(either by legitimately logging into the system or by exploiting some other
service on the system) can execute arbitrary code with the privileges of
the user running the telnet daemon (usually root).

IV.  Workaround

No workaround is available, but systems which are not running the telnet
daemon are not vulnerable.

V.   Solution

Perform one of the following:

1) Upgrade your vulnerable system to 7-STABLE, or to the RELENG_7_1 or
```

RELENG_7_0 security branch dated after the correction date.

2) To patch your present system:

The following patches have been verified to apply to FreeBSD 7.0 and 7.1 systems.

a) Download the relevant patch from the location below, and verify the detached PGP signature using your PGP utility.

```
# fetch http://security.FreeBSD.org/patches/SA-09:05/telnetd.patch
# fetch http://security.FreeBSD.org/patches/SA-09:05/telnetd.patch.asc
```

b) Execute the following commands as root:

```
# cd /usr/src
# patch < /path/to/patch
# cd /usr/src/lib/libtelnet
# make obj && make depend && make
# cd /usr/src/libexec/telnetd
# make obj && make depend && make && make install
```

VI. Correction details

The following list contains the revision numbers of each file that was corrected in FreeBSD.

CVS:

```
Branch                                                           Revision
  Path
- -------------------------------------------------------------------------
RELENG_7
  src/contrib/telnet/telnetd/sys_term.c                         1.18.22.1
RELENG_7_1
  src/UPDATING                                             1.507.2.13.2.6
  src/sys/conf/newvers.sh                                    1.72.2.9.2.7
  src/contrib/telnet/telnetd/sys_term.c                         1.18.30.2
RELENG_7_0
  src/UPDATING                                             1.507.2.3.2.14
  src/sys/conf/newvers.sh                                   1.72.2.5.2.14
  src/contrib/telnet/telnetd/sys_term.c                         1.18.26.1
- -------------------------------------------------------------------------
```

Subversion:

```
Branch/path                                                      Revision
- -------------------------------------------------------------------------
stable/7/                                                         r188699
releng/7.1/                                                       r188699
releng/7.0/                                                       r188699
- -------------------------------------------------------------------------
```

VII. References

http://lists.grok.org.uk/pipermail/full-disclosure/2009-February/067954.html

The latest revision of this advisory is available at
http://security.FreeBSD.org/advisories/FreeBSD-SA-09:05.telnetd.asc

```
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.9 (FreeBSD)

iEYEARECAAYFAkmZ5xkACgkQFdaIBMps37L1/gCgid6+mQr/h3kHKq6bUL8TW+St
TBUAoIFSFbE0PsTtt1nrwlSAZwvvDL0s
=y6p4
-----END PGP SIGNATURE-----
```

To implement this advisory, we follow the instructions in part 2.

```
freebsd7# fetch http://security.FreeBSD.org/patches/SA-09:05/telnetd.patch
telnetd.patch
                               100% of 1010  B  280 kBps
freebsd7# fetch http://security.FreeBSD.org/patches/SA-09:05/telnetd.patch.asc
telnetd.patch.asc                              100% of  195  B   53 kBps

freebsd7# gpg --verify telnetd.patch.asc telnetd.patch
gpg: Signature made Mon Feb 16 16:30:19 2009 EST using DSA key ID CA6CDFB2
gpg: Good signature from "FreeBSD Security Officer <security-officer@FreeBSD.org>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: C374 0FC5 69A6 FBB1 4AED  B131 15D6 8804 CA6C DFB2

freebsd7# cd /usr/src
freebsd7# patch < /root/telnetd.patch
Hmm...  Looks like a unified diff to me...
The text leading up to this was:
--------------------------
|Index: contrib/telnet/telnetd/sys_term.c
|===================================================================
|--- contrib/telnet/telnetd/sys_term.c  (revision 188667)
|+++ contrib/telnet/telnetd/sys_term.c  (working copy)
--------------------------
Patching file contrib/telnet/telnetd/sys_term.c using Plan A...
Hunk #1 succeeded at 1285 (offset 14 lines).
Hunk #2 succeeded at 1310 (offset 14 lines).
done

freebsd7# cd /usr/src/lib/libtelnet

freebsd7# make obj && make depend && make

/usr/obj/usr/src/lib/libtelnet created for /usr/src/lib/libtelnet
rm -f .depend
mkdep -f .depend -a    -I/usr/src/lib/libtelnet/../../contrib/telnet -DENCRYPTION -DAUTHENTICATION -DSRA -
DKRB5 -I/lib/krb5 -I -I -DFORWARD -Dnet_write=telnet_net_write /usr/src/lib/libtelnet/../../contrib/
telnet/libtelnet/genget.c /usr/src/lib/libtelnet/../../contrib/telnet/libtelnet/getent.c /usr/src/lib/
libtelnet/../../contrib/telnet/libtelnet/misc.c /usr/src/lib/libtelnet/../../contrib/telnet/libtelnet/
encrypt.c /usr/src/lib/libtelnet/../../contrib/telnet/libtelnet/auth.c /usr/src/lib/libtelnet/../../
contrib/telnet/libtelnet/enc_des.c /usr/src/lib/libtelnet/../../contrib/telnet/libtelnet/sra.c /usr/src/
lib/libtelnet/../../contrib/telnet/libtelnet/pk.c /usr/src/lib/libtelnet/../../contrib/telnet/libtelnet/
kerberos5.c
...edited...
building static telnet library
ranlib libtelnet.a

freebsd7# cd /usr/src/libexec/telnetd

freebsd7# make obj && make depend && make && make install
/usr/obj/usr/src/libexec/telnetd created for /usr/src/libexec/telnetd
rm -f .depend
mkdep -f .depend -a    -DLINEMODE -DUSE_TERMIO -DDIAGNOSTICS -DOLD_ENVIRON -DENV_HACK -DINET6 -I/usr/src/
libexec/telnetd/../../contrib/telnet -DAUTHENTICATION -DENCRYPTION -DKRB5 -DFORWARD -
Dnet_write=telnet_net_write /usr/src/libexec/telnetd/../../contrib/telnet/telnetd/global.c /usr/src/
libexec/telnetd/../../contrib/telnet/telnetd/slc.c /usr/src/libexec/telnetd/../../contrib/telnet/telnetd/
state.c /usr/src/libexec/telnetd/../../contrib/telnet/telnetd/sys_term.c /usr/src/libexec/telnetd/../../
contrib/telnet/telnetd/telnetd.c /usr/src/libexec/telnetd/../../contrib/telnet/telnetd/termstat.c /usr/
src/libexec/telnetd/../../contrib/telnet/telnetd/utility.c /usr/src/libexec/telnetd/../../contrib/telnet/
telnetd/authenc.c
...edited...
install -s -o root -g wheel -m 555   telnetd /usr/libexec
install -o root -g wheel -m 444 telnetd.8.gz  /usr/share/man/man8
```

Since telnetd runs from inetd, we can be sure the next time telnetd starts it will be patched.

In the previous edition of this document (published in 2005), we provided an example of manually patching the userland for FreeBSD-SA-04:05.openssl. That advisory required recompiling the entire userland. The same is true for FreeBSD-SA-06:23.openssl. However, there does not seem to be an advisory since 2006 that required recompiling the whole userland. Even FreeBSD-SA-09:08.openssl, another OpenSSL advisory, only required recompiling part of the userland, as was the case with this telnetd example. In the event you wish to apply a userland patch manually, and it requires recompiling the userland, follow the instructions in the advisory as we have done with these last two examples.

Using CVSup to Apply Patches

So far we have shown how to do quick binary updates using FreeBSD Update, and we manually applied a kernel patch and then a userland patch. In this example we will use the traditional CVSup tool to update the entire system to a specific point in time. For this example we will use the FreeBSD-SA-09:07.libc security advisory (http://security.freebsd.org/advisories/FreeBSD-SA-09:07.libc.asc) to guide our actions.

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

=============================================================================
FreeBSD-SA-09:07.libc                                       Security Advisory
                                                          The FreeBSD Project

Topic:          Information leak in db(3)

Category:       core
Module:         libc
Announced:      2009-04-22
Credits:        Jaakko Heinonen, Xin LI
Affects:        All supported versions of FreeBSD.
Corrected:      2009-04-11 15:19:26 UTC (RELENG_7, 7.2-PRERELEASE)
                2009-04-22 14:07:14 UTC (RELENG_7_1, 7.1-RELEASE-p5)
                2009-04-22 14:07:14 UTC (RELENG_7_0, 7.0-RELEASE-p12)
                2009-04-11 15:21:11 UTC (RELENG_6, 6.4-STABLE)
                2009-04-22 14:07:14 UTC (RELENG_6_4, 6.4-RELEASE-p4)
                2009-04-22 14:07:14 UTC (RELENG_6_3, 6.3-RELEASE-p10)

For general information regarding FreeBSD Security Advisories,
including descriptions of the fields above, security branches, and the
following sections, please visit <URL:http://security.FreeBSD.org/>.

I.   Background

FreeBSD's C library (libc) contains code for creating and accessing
Berkeley DB 1.85 database files.  Such databases are used extensively
in FreeBSD; for example, the system password files (/etc/passwd and
/etc/master.passwd) are normally accessed via their database files
(/etc/pwd.db and /etc/spwd.db).

II.  Problem Description

Some data structures used by the database interface code are not properly
initialized when allocated.

III. Impact

Programs using the db(3) interface to create Berkeley database files may
"leak" sensitive information into database files.  If those files can be
read by other users, this may result in the disclosure of sensitive
information such as login credentials.

IV.  Workaround

No workaround is available, but systems without untrusted local users are
probably not affected (since remote attackers will in most cases not be
able to read such database files).
```

V.   Solution

Perform one of the following:

1) Upgrade your vulnerable system to 6-STABLE, or 7-STABLE, or to the RELENG_7_1, RELENG_7_0, RELENG_6_4, or RELENG_6_3 security branch dated after the correction date.

2) To patch your present system:

The following patches have been verified to apply to FreeBSD 6.3, 6.4, 7.0, and 7.1 systems.

a) Download the relevant patch from the location below, and verify the detached PGP signature using your PGP utility.

```
# fetch http://security.FreeBSD.org/patches/SA-09:07/libc.patch
# fetch http://security.FreeBSD.org/patches/SA-09:07/libc.patch.asc
```

b) Execute the following commands as root:

```
# cd /usr/src
# patch < /path/to/patch
# cd /usr/src/lib/libc
# make obj &amp;&amp; make depend &amp;&amp; make &amp;&amp; make install
```

NOTE: On the amd64 platform, the above procedure will not update the lib32 (i386 compatibility) libraries. On amd64 systems where the i386 compatibility libraries are used, the operating system should instead be recompiled as described in <URL:http://www.FreeBSD.org/handbook/makeworld.html>

NOTE: System administrators may wish to rebuild any system database files which were created prior to applying this patch in case they contain sensitive information.

VI. Correction details

The following list contains the revision numbers of each file that was corrected in FreeBSD.

CVS:

```
Branch                                                           Revision
  Path
- -------------------------------------------------------------------------
RELENG_6
  src/lib/libc/db/btree/bt_split.c                                1.7.2.1
...edited...
RELENG_7
  src/lib/libc/db/btree/bt_split.c                                1.8.2.1
  src/lib/libc/db/btree/bt_open.c                                1.12.2.1
  src/lib/libc/db/hash/hash_buf.c                                 1.8.2.1
  src/lib/libc/db/mpool/mpool.c                                  1.13.2.1
  src/lib/libc/db/README                                         1.1.50.1
RELENG_7_1
  src/UPDATING                                             1.507.2.13.2.8
  src/sys/conf/newvers.sh                                    1.72.2.9.2.9
  src/lib/libc/db/btree/bt_split.c                                1.8.6.2
  src/lib/libc/db/hash/hash_buf.c                                 1.8.6.2
  src/lib/libc/db/mpool/mpool.c                                  1.13.6.2
RELENG_7_0
  src/UPDATING                                             1.507.2.3.2.16
  src/sys/conf/newvers.sh                                   1.72.2.5.2.16
  src/lib/libc/db/btree/bt_split.c                                1.8.4.1
  src/lib/libc/db/hash/hash_buf.c                                 1.8.4.1
  src/lib/libc/db/mpool/mpool.c                                  1.13.4.1
```

```
- -------------------------------------------------------------------------

Subversion:

Branch/path                                                      Revision
- -------------------------------------------------------------------------
stable/6/                                                         r190940
releng/6.4/                                                       r191381
releng/6.3/                                                       r191381
stable/7/                                                         r190939
releng/7.1/                                                       r191381
releng/7.0/                                                       r191381
- -------------------------------------------------------------------------

The latest revision of this advisory is available at
http://security.FreeBSD.org/advisories/FreeBSD-SA-09:07.libc.asc
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.9 (FreeBSD)

iEYEARECAAYFAknvJlkACgkQFdaIBMps37JcyACggmDk96JTy3G5gGlzMlNuVsV7
s5wAoIT2G2c3T6bYa7GeftWLpGGFo2Rp
=rdqD
-----END PGP SIGNATURE-----
```

This security advisory requires a patch to libc. We could have user binary updates to fix this, or applied the security patch manually. Instead we are going to update the whole system to a time when the patch was integrated into the FreeBSD source tree. This is "Solution 1" in the advisory. We take the time from the "Corrected" section of the advisory. Because our system is running FreeBSD 7.1, we look for the date involving that version of FreeBSD.

```
2009-04-22 14:07:14 UTC (RELENG_7_1, 7.1-RELEASE-p5)
```

This means we can update all of the source code on our system to a date after 2009-04-22 14:07:14 UTC to be sure the libc patch is applied.

In order to do that, we will use CVSup. We need to create a "supfile" that controls how CVSup operates. Examples are on the system already:

```
freebsd7# ls /usr/share/examples/cvsup
README                  ports-supfile           standard-supfile
cvs-supfile             refuse                  www-supfile
doc-supfile             refuse.README
gnats-supfile           stable-supfile
```

We create our own file with these contents:

```
freebsd7# cat /usr/local/etc/freebsd7-example.supfile
*default host=INSERTYOURCHOICE.FreeBSD.org
*default base=/usr
*default prefix=/usr
*default release=cvs tag=RELENG_7_1
*default delete use-rel-suffix
*default date=2009.04.22.14.08.00
*default compress
src-all
```

Please replace INSERTYOURCHOICE.FreeBSD.org in this and later occurrences with the hostname of a real CVSup server as listed in the FreeBSD Handbook (http://www.freebsd.org/doc/en/books/handbook/cvsup.html).

We set the date to be in the minute after the correction time noted earlier.

Now we are ready to use CVSup to update our source tree.

```
freebsd7# cvsup -g -L 2 /usr/local/etc/freebsd7-example.supfile
Parsing supfile "/usr/local/etc/freebsd7-example.supfile"
Connecting to cvsup3.FreeBSD.org
Connected to cvsup3.FreeBSD.org
```

```
Server software version: SNAP_16_1h
Negotiating file attribute support
Exchanging collection information
Establishing multiplexed-mode data connection
Running
Updating collection src-all/cvs
 Edit src/UPDATING
  Add delta 1.507.2.13.2.4 2009.01.07.20.17.55 simon
  Add delta 1.507.2.13.2.5 2009.01.13.21.19.27 simon
  Add delta 1.507.2.13.2.6 2009.02.16.21.56.17 cperciva
  Add delta 1.507.2.13.2.7 2009.03.23.00.00.50 cperciva
  Add delta 1.507.2.13.2.8 2009.04.22.14.07.14 cperciva
 Edit src/contrib/bind9/lib/dns/openssldsa_link.c
  Add delta 1.1.1.3.2.1.4.1 2009.01.13.21.19.27 simon
 Edit src/contrib/bind9/lib/dns/opensslrsa_link.c
  Add delta 1.1.1.4.6.1 2009.01.13.21.19.27 simon
...edited...
 SetAttrs src/usr.sbin/pkg_install/tkpkg,v
Shutting down connection to server
Finished successfully
```

Notice the last date listed for updates to src/UPDATING is less than the time specified in our supfile. There are no updates beyond 2009-04-22 14:07:14 UTC. This means CVSup is working as expected. In other words, we are getting updates to 7.1 RELEASE, but not newer than our specified correction date.

Note that CVSup does not natively support HTTP proxies. For information on how to use CVSup through a proxy, specifically mentioning FreeBSD, see my blog post Updating FreeBSD Using CVSup through HTTP Proxy (http://taosecurity.blogspot.com/2009/08/updating-freebsd-using-cvsup-through.html).

```
cd /usr/src
make buildworld
make buildkernel KERNCONF=FREEBSD7
make installkernel KERNCONF=FREEBSD7
mergemaster -p
make installworld
mergemaster
reboot
```

Note in the following output, that when asked whether to install a change using the 'i' input, we usually answer yes. The main exception invovles overwriting files used for authentication, like /etc/passwd. In the event a file like that is overwritten, the administrator can log in at the console as root (with no password), and then manually reinstall user accounts and set passwords.

In the following example, we do NOT install the file provided by the upgrade, because doing so would delete our /etc/master.passwd file.

```
-# $FreeBSD: src/etc/master.passwd,v 1.40.18.1 2008/11/25 02:59:29 kensmith Exp $
+# $FreeBSD: src/etc/master.passwd,v 1.40 2005/06/06 20:19:56 brooks Exp $
 #
-root:$1$GblWCfv6$O..51HNClSYy5aEgE43Lx/:0:0::0:0:Charlie &:/root:/bin/csh
+root::0:0::0:0:Charlie &:/root:/bin/csh
 toor:*:0:0::0:0:Bourne-again Superuser:/root:
 daemon:*:1:1::0:0:Owner of many system processes:/root:/usr/sbin/nologin
 operator:*:2:5::0:0:System &:/:/usr/sbin/nologin
@@ -21,4 +21,3 @@
 pop:*:68:6::0:0:Post Office Owner:/nonexistent:/usr/sbin/nologin
 www:*:80:80::0:0:World Wide Web Owner:/nonexistent:/usr/sbin/nologin
 nobody:*:65534:65534::0:0:Unprivileged user:/nonexistent:/usr/sbin/nologin
-analyst:$1$FNYoY3Rk$lLVv/eHHIuLpz0AEAAYxO/:1001:1001::0:0:analyst:/home/analyst:/bin/sh

  Use 'd' to delete the temporary ./etc/master.passwd
  Use 'i' to install the temporary ./etc/master.passwd
  Use 'm' to merge the temporary and installed versions
  Use 'v' to view the diff results again

  Default is to leave the temporary file to deal with by hand
```

```
How should I deal with this? [Leave it for later] d
```

An alternative to deleting the temporary file and not accepting changes is to manually integrate changes to files. See the FreeBSD Handbook for information on that process.

In the following we show sample output from the entire update process.

```
freebsd7# cd /usr/src
freebsd7# make buildworld
--------------------------------------------------------------
>>> World build started on Fri Aug 21 09:15:41 EDT 2009
--------------------------------------------------------------

--------------------------------------------------------------
>>> Rebuilding the temporary build tree
--------------------------------------------------------------
rm -rf /usr/obj/usr/src/tmp
mkdir -p /usr/obj/usr/src/tmp/legacy/usr/bin
mkdir -p /usr/obj/usr/src/tmp/legacy/usr/games
...edited...
===> etc/sendmail (all)
rm -f freebsd.cf
m4 -D_CF_DIR_=/usr/src/etc/sendmail/../../contrib/sendmail/cf/   /usr/src/etc/sendmail/../../contrib/
sendmail/cf/m4/cf.m4 /usr/src/etc/sendmail/freebsd.mc > freebsd.cf
chmod 444 freebsd.cf
rm -f freebsd.submit.cf
m4 -D_CF_DIR_=/usr/src/etc/sendmail/../../contrib/sendmail/cf/   /usr/src/etc/sendmail/../../contrib/
sendmail/cf/m4/cf.m4 /usr/src/etc/sendmail/freebsd.submit.mc > freebsd.submit.cf
chmod 444 freebsd.submit.cf

--------------------------------------------------------------
>>> World build completed on Fri Aug 21 12:34:00 EDT 2009
--------------------------------------------------------------

freebsd7# make buildkernel KERNCONF=FREEBSD7

--------------------------------------------------------------
>>> Kernel build for FREEBSD7 started on Fri Aug 21 12:34:28 EDT 2009
--------------------------------------------------------------
===> FREEBSD7
mkdir -p /usr/obj/usr/src/sys

--------------------------------------------------------------
>>> stage 1: configuring the kernel
--------------------------------------------------------------
...edited...
ld -Bshareable  -d -warn-common -o if_zyd.ko.debug if_zyd.kld
objcopy --only-keep-debug if_zyd.ko.debug if_zyd.ko.symbols
objcopy --strip-debug --add-gnu-debuglink=if_zyd.ko.symbols if_zyd.ko.debug if_zyd.ko
--------------------------------------------------------------
>>> Kernel build for FREEBSD7 completed on Fri Aug 21 13:35:05 EDT 2009
--------------------------------------------------------------

freebsd7# make installkernel KERNCONF=FREEBSD7
--------------------------------------------------------------
>>> Installing kernel
--------------------------------------------------------------
cd /usr/obj/usr/src/sys/FREEBSD7;  MAKEOBJDIRPREFIX=/usr/obj  MACHINE_ARCH=i386
...edited...
install -o root -g wheel -m 555   if_zyd.ko.symbols /boot/kernel
kldxref /boot/kernel

freebsd7# mergemaster -p
*** Unable to find mtree database. Skipping auto-upgrade.

*** Creating the temporary root environment in /var/tmp/temproot
```

```
 *** /var/tmp/temproot ready for use
 *** Creating and populating directory structure in /var/tmp/temproot



*** Beginning comparison

 *** Temp ./etc/master.passwd and installed have the same CVS Id, deleting
 *** Temp ./etc/group and installed have the same CVS Id, deleting

*** Comparison complete

Do you wish to delete what is left of /var/tmp/temproot? [no]
 *** /var/tmp/temproot will remain

grep: /etc/make.conf: No such file or directory

*** Comparing make variables

*** From /etc/make.conf
*** From /usr/src/share/examples/etc/make.conf

freebsd7# make installworld
mkdir -p /tmp/install.fsulHZM5
for prog in [ awk cap_mkdb cat chflags chmod chown  date echo egrep find grep install-info  ln lockf make
mkdir mtree mv pwd_mkdb rm sed sh sysctl  test true uname wc zic; do  cp `which $prog` /tmp/
install.fsulHZM5;  done
...edited...
===> etc/sendmail (install)
cd /usr/src/etc/../share/man; make makedb
makewhatis /usr/share/man
makewhatis /usr/share/openssl/man
rm -rf /tmp/install.fsulHZM5

freebsd7# mergemaster
*** Unable to find mtree database. Skipping auto-upgrade.

*** The directory specified for the temporary root environment,
    /var/tmp/temproot, exists.  This can be a security risk if untrusted
    users have access to the system.

  Use 'd' to delete the old /var/tmp/temproot and continue
  Use 't' to select a new temporary root directory
  Use 'e' to exit mergemaster

  Default is to use /var/tmp/temproot as is

How should I deal with this? [Use the existing /var/tmp/temproot]

   *** Leaving /var/tmp/temproot intact

*** Creating the temporary root environment in /var/tmp/temproot
 *** /var/tmp/temproot ready for use
 *** Creating and populating directory structure in /var/tmp/temproot

mtree -eU  -f /usr/src/etc/mtree/BSD.root.dist -p /var/tmp/temproot/
./bin missing (created)
./boot missing (created)
./boot/defaults missing (created)
...edited...
 *** Temp ./etc/login.access and installed have the same CVS Id, deleting
 *** Temp ./etc/login.conf and installed have the same CVS Id, deleting
 *** Temp ./etc/mac.conf and installed have the same CVS Id, deleting

   ======================================================================

  *** Displaying differences between ./etc/motd and installed version:
```

```
--- /etc/motd   2009-08-21 08:49:15.000000000 -0400
+++ ./etc/motd  2009-08-21 13:51:40.000000000 -0400
@@ -1,4 +1,4 @@
-FreeBSD 7.1-RELEASE (GENERIC) #0: Thu Jan  1 14:37:25 UTC 2009
+FreeBSD ?.?.?  (UNKNOWN)

 Welcome to FreeBSD!


  Use 'd' to delete the temporary ./etc/motd
  Use 'i' to install the temporary ./etc/motd
  Use 'm' to merge the temporary and installed versions
  Use 'v' to view the diff results again

  Default is to leave the temporary file to deal with by hand

How should I deal with this? [Leave it for later] i


   *** ./etc/motd installed successfully

 *** Temp ./etc/netconfig and installed have the same CVS Id, deleting
 *** Temp ./etc/network.subr and installed have the same CVS Id, deleting
...edited...
 *** Temp ./.profile and installed have the same CVS Id, deleting
 *** Temp ./COPYRIGHT and installed have the same CVS Id, deleting

*** Comparison complete
*** Saving mtree database for future upgrades

Do you wish to delete what is left of /var/tmp/temproot? [no]
 *** /var/tmp/temproot will remain

freebsd7# reboot

freebsd7# uname -a
FreeBSD freebsd7.localdomain 7.1-RELEASE-p5 FreeBSD 7.1-RELEASE-p5 #0: Fri Aug 21 12:59:27 EDT 2009
root@freebsd7.localdomain:/usr/obj/usr/src/sys/FREEBSD7  i386
```

The system is now completely updated to the time specified in the supfile. However, the compilation date for the kernel shows when the kernel was compiled.

Using Csup to Apply Patches

In the last example we used the traditional CVSup tool to apply patches to a system. Most FreeBSD administrators are very familiar with using that tool. However, since FreeBSD 6.2, a C replacement called Csup by Maxime Henrion has been available. In this example we will use the new Csup tool to update the entire system to a specific point in time. For this example we will use the FreeBSD-SA-09:09.pipe.asc security advisory (http://security.freebsd.org/advisories/FreeBSD-SA-09:09.pipe.asc) to guide our actions.

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

=============================================================================
FreeBSD-SA-09:09.pipe                                       Security Advisory
                                                          The FreeBSD Project

Topic:          Local information disclosure via direct pipe writes

Category:       core
Module:         kern
Announced:      2009-06-10
Credits:        Pieter de Boer
Affects:        All supported versions of FreeBSD.
```

```
Corrected:      2009-06-10 10:31:11 UTC (RELENG_7, 7.2-STABLE)
                2009-06-10 10:31:11 UTC (RELENG_7_2, 7.2-RELEASE-p1)
                2009-06-10 10:31:11 UTC (RELENG_7_1, 7.1-RELEASE-p6)
                2009-06-10 10:31:11 UTC (RELENG_6, 6.4-STABLE)
                2009-06-10 10:31:11 UTC (RELENG_6_4, 6.4-RELEASE-p5)
                2009-06-10 10:31:11 UTC (RELENG_6_3, 6.3-RELEASE-p11)
```

For general information regarding FreeBSD Security Advisories, including descriptions of the fields above, security branches, and the following sections, please visit <URL:http://security.FreeBSD.org/>.

I.   Background

One of the most commonly used forms of interprocess communication on FreeBSD and other UNIX-like systems is the (anonymous) pipe. In this mechanism, a pair of file descriptors is created, and data written to one descriptor can be read from the other.

FreeBSD's pipe implementation contains an optimization known as "direct writes". In this optimization, rather than copying data into kernel memory when the write(2) system call is invoked and then copying the data again when the read(2) system call is invoked, the FreeBSD kernel takes advantage of virtual memory mapping to allow the data to be copied directly between processes.

II. Problem Description

An integer overflow in computing the set of pages containing data to be copied can result in virtual-to-physical address lookups not being performed.

III. Impact

An unprivileged process can read pages of memory which belong to other processes or to the kernel. These may contain information which is sensitive in itself; or may contain passwords or cryptographic keys which can be indirectly exploited to gain sensitive information or access.

IV. Workaround

No workaround is available, but systems without untrusted local users are not vulnerable. System administrators are reminded that even if a system is not intended to have untrusted local users, it may be possible for an attacker to exploit some other vulnerability to obtain local user access to a system.

V.   Solution

Perform one of the following:

1) Upgrade your vulnerable system to 6-STABLE, or 7-STABLE, or to the RELENG_7_2, RELENG_7_1, RELENG_6_4, or RELENG_6_3 security branch dated after the correction date.

2) To patch your present system:

The following patches have been verified to apply to FreeBSD 6.3, 6.4, 7.1, and 7.2 systems.

a) Download the relevant patch from the location below, and verify the detached PGP signature using your PGP utility.

```
# fetch http://security.FreeBSD.org/patches/SA-09:09/pipe.patch
# fetch http://security.FreeBSD.org/patches/SA-09:09/pipe.patch.asc
```

b) Apply the patch.

```
# cd /usr/src
# patch < /path/to/patch
```

c) Recompile your kernel as described in
<URL:http://www.FreeBSD.org/handbook/kernelconfig.html> and reboot the
system.

VI. Correction details

The following list contains the revision numbers of each file that was
corrected in FreeBSD.

CVS:

```
Branch                                                           Revision
  Path
- -------------------------------------------------------------------------
RELENG_6
  src/sys/kern/sys_pipe.c                                       1.184.2.5
...edited...
RELENG_7
  src/sys/kern/sys_pipe.c                                       1.191.2.5
RELENG_7_2
  src/UPDATING                                             1.507.2.23.2.4
  src/sys/conf/newvers.sh                                   1.72.2.11.2.5
  src/sys/kern/sys_pipe.c                                   1.191.2.3.4.2
RELENG_7_1
  src/UPDATING                                             1.507.2.13.2.9
  src/sys/conf/newvers.sh                                   1.72.2.9.2.10
  src/sys/kern/sys_pipe.c                                   1.191.2.3.2.2
- -------------------------------------------------------------------------
```

Subversion:

```
Branch/path                                                      Revision
- -------------------------------------------------------------------------
stable/6/                                                         r193893
releng/6.4/                                                       r193893
releng/6.3/                                                       r193893
stable/7/                                                         r193893
releng/7.2/                                                       r193893
releng/7.1/                                                       r193893
- -------------------------------------------------------------------------
```

VII. References

The latest revision of this advisory is available at
http://security.FreeBSD.org/advisories/FreeBSD-SA-09:09.pipe.asc

```
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.9 (FreeBSD)

iEYEARECAAYFAkovjN0ACgkQFdaIBMps37JkXwCgmLcEMOMAEIXRoJ220zwZhMKn
f+gAn1bZyLMhfZU7TI0xxhizwetDwMVI
=J37B
-----END PGP SIGNATURE-----
```

This security advisory requires a patch to the kernel. We could have user binary updates to fix this, or applied the security patch manually. Instead we are going to update the whole system to a time when the patch was integrated into the FreeBSD source tree. This is "Solution 1" in the advisory. We take the time from the "Corrected" section of the advisory. Because our system is running FreeBSD 7.1, we look for the date involving that version of FreeBSD.

2009-06-10 10:31:11 UTC (RELENG_7_1, 7.1-RELEASE-p6)

This means we can update all of the source code on our system to a date after 2009-06-10 10:31:11 UTC to be sure the kernel patch is applied.

In order to do that, we will use Csup. We will modify our earlier supfile that controls how Csup operates.

```
freebsd7# cat /usr/local/etc/freebsd7-example.supfile
*default host=INSERTYOURCHOICE.FreeBSD.org
*default base=/usr
*default prefix=/usr
*default release=cvs tag=RELENG_7_1
*default delete use-rel-suffix
*default date=2009.06.10.10.32.00
*default compress
src-all
```

We set the date to be in the minute after the correction time noted earlier.

Now we are ready to use Csup to update our source tree.

```
freebsd7# csup -g -L 2 /usr/local/etc/freebsd7-example.supfile
Parsing supfile "/usr/local/etc/freebsd7-example.supfile"
Connecting to cvsup3.FreeBSD.org
Connected to 128.31.0.28
Server software version: SNAP_16_1h
Negotiating file attribute support
Exchanging collection information
Establishing multiplexed-mode data connection
Running
Updating collection src-all/cvs
 Edit src/UPDATING
  Add delta 1.507.2.13.2.9 2009.06.10.10.31.11 cperciva
 Edit src/contrib/ntp/ntpd/ntp_crypto.c
  Add delta 1.1.1.3.18.1.2.2 2009.06.10.10.31.11 cperciva
 Edit src/sys/conf/newvers.sh
  Add delta 1.72.2.9.2.10 2009.06.10.10.31.11 cperciva
 Edit src/sys/kern/sys_pipe.c
  Add delta 1.191.2.3.2.2 2009.06.10.10.31.11 cperciva
 Edit src/sys/netinet6/in6.c
  Add delta 1.73.2.4.2.2 2009.06.10.10.31.11 cperciva
Shutting down connection to server
Finished successfully
```

Now we can follow the same process as seen in the previous example.

```
cd /usr/src
make buildworld
make buildkernel KERNCONF=FREEBSD7
make installkernel KERNCONF=FREEBSD7
mergemaster -p
make installworld
mergemaster
reboot
```

```
freebsd7# cd /usr/src
freebsd7# make buildworld
--------------------------------------------------------------
>>> World build started on Fri Aug 21 14:32:14 EDT 2009
--------------------------------------------------------------

--------------------------------------------------------------
>>> Rebuilding the temporary build tree
--------------------------------------------------------------
rm -rf /usr/obj/usr/src/tmp
mkdir -p /usr/obj/usr/src/tmp/legacy/usr/bin
mkdir -p /usr/obj/usr/src/tmp/legacy/usr/games
...edited...
chmod 444 freebsd.cf
rm -f freebsd.submit.cf
```

```
m4 -D_CF_DIR_=/usr/src/etc/sendmail/../../contrib/sendmail/cf/   /usr/src/etc/sendmail/../../contrib/
sendmail/cf/m4/cf.m4 /usr/src/etc/sendmail/freebsd.submit.mc > freebsd.submit.cf
chmod 444 freebsd.submit.cf

--------------------------------------------------------------
>>> World build completed on Fri Aug 21 17:48:17 EDT 2009
--------------------------------------------------------------

freebsd7# make buildkernel KERNCONF=FREEBSD7

--------------------------------------------------------------
>>> Kernel build for FREEBSD7 started on Fri Aug 21 19:10:33 EDT 2009
--------------------------------------------------------------
===> FREEBSD7
mkdir -p /usr/obj/usr/src/sys

--------------------------------------------------------------
>>> stage 1: configuring the kernel
--------------------------------------------------------------
cd /usr/src/sys/i386/conf;  PATH=/usr/obj/usr/src/tmp/legacy/usr/sbin:/usr/obj/usr/src/tmp/legacy/usr/
bin:/usr/obj/usr/src/tmp/legacy/usr/games:/usr/obj/usr/src/tmp/usr/sbin:/usr/obj/usr/src/tmp/usr/bin:/usr/
obj/usr/src/tmp/usr/games:/sbin:/bin:/usr/sbin:/usr/bin  config  -d /usr/obj/usr/src/sys/FREEBSD7  /usr/
src/sys/i386/conf/FREEBSD7
...edited...
objcopy --strip-debug --add-gnu-debuglink=if_zyd.ko.symbols if_zyd.ko.debug if_zyd.ko
--------------------------------------------------------------
>>> Kernel build for FREEBSD7 completed on Fri Aug 21 20:11:01 EDT 2009
--------------------------------------------------------------

freebsd7# make installkernel KERNCONF=FREEBSD7
--------------------------------------------------------------
>>> Installing kernel
--------------------------------------------------------------
cd /usr/obj/usr/src/sys/FREEBSD7;  MAKEOBJDIRPREFIX=/usr/obj  MACHINE_ARCH=i386  MACHINE=i386  CPUTYPE=
GROFF_BIN_PATH=/usr/obj/usr/src/tmp/legacy/usr/bin  GROFF_FONT_PATH=/usr/obj/usr/src/tmp/legacy/usr/share/
groff_font  GROFF_TMAC_PATH=/usr/obj/usr/src/tmp/legacy/usr/share/tmac PATH=/usr/obj/usr/src/tmp/legacy/
usr/sbin:/usr/obj/usr/src/tmp/legacy/usr/bin:/usr/obj/usr/src/tmp/legacy/usr/games:/usr/obj/usr/src/tmp/
usr/sbin:/usr/obj/usr/src/tmp/usr/bin:/usr/obj/usr/src/tmp/usr/games:/sbin:/bin:/usr/sbin:/usr/bin  make
KERNEL=kernel install
thiskernel=`sysctl -n kern.bootfile` ;  if [ ! "`dirname "$thiskernel"`" -ef /boot/kernel ] ; then
chflags -R noschg /boot/kernel ;  rm -rf /boot/kernel ;  else  if [ -d /boot/kernel.old ] ; then  chflags
-R noschg /boot/kernel.old ;  rm -rf /boot/kernel.old ;  fi ;  mv /boot/kernel /boot/kernel.old ;  sysctl
kern.bootfile=/boot/kernel.old/"`basename "$thiskernel"`" ;  fi
kern.bootfile: /boot/kernel/kernel -> /boot/kernel.old/kernel
mkdir -p /boot/kernel
install -p -m 555 -o root -g wheel kernel /boot/kernel
install -p -m 555 -o root -g wheel kernel.symbols /boot/kernel
...edited...
install -o root -g wheel -m 555   if_zyd.ko /boot/kernel
install -o root -g wheel -m 555   if_zyd.ko.symbols /boot/kernel
kldxref /boot/kernel

freebsd7# mergemaster -p

*** The directory specified for the temporary root environment,
    /var/tmp/temproot, exists.  This can be a security risk if untrusted
    users have access to the system.

  Use 'd' to delete the old /var/tmp/temproot and continue
  Use 't' to select a new temporary root directory
  Use 'e' to exit mergemaster

  Default is to use /var/tmp/temproot as is

How should I deal with this? [Use the existing /var/tmp/temproot]

   *** Leaving /var/tmp/temproot intact
*** Creating the temporary root environment in /var/tmp/temproot
 *** /var/tmp/temproot ready for use
 *** Creating and populating directory structure in /var/tmp/temproot



*** Beginning comparison

 *** Temp ./etc/master.passwd and installed have the same CVS Id, deleting
 *** Temp ./etc/group and installed have the same CVS Id, deleting

*** Comparison complete

Do you wish to delete what is left of /var/tmp/temproot? [no]
 *** /var/tmp/temproot will remain

grep: /etc/make.conf: No such file or directory

*** Comparing make variables

*** From /etc/make.conf
*** From /usr/src/share/examples/etc/make.conf

freebsd7# make installworld
mkdir -p /tmp/install.CQb9zEn9
for prog in [ awk cap_mkdb cat chflags chmod chown  date echo egrep find grep install-info  ln lockf make
mkdir mtree mv pwd_mkdb rm sed sh sysctl  test true uname wc zic; do  cp `which $prog` /tmp/
install.CQb9zEn9;  done
cd /usr/src; MAKEOBJDIRPREFIX=/usr/obj  MACHINE_ARCH=i386  MACHINE=i386  CPUTYPE=  GROFF_BIN_PATH=/usr/
obj/usr/src/tmp/legacy/usr/bin  GROFF_FONT_PATH=/usr/obj/usr/src/tmp/legacy/usr/share/groff_font
GROFF_TMAC_PATH=/usr/obj/usr/src/tmp/legacy/usr/share/tmac  PATH=/usr/obj/usr/src/tmp/legacy/usr/sbin:/
usr/obj/usr/src/tmp/legacy/usr/bin:/usr/obj/usr/src/tmp/legacy/usr/games:/usr/obj/usr/src/tmp/usr/sbin:/
usr/obj/usr/src/tmp/usr/bin:/usr/obj/usr/src/tmp/usr/games:/tmp/install.CQb9zEn9 make -f Makefile.inc1
reinstall
--------------------------------------------------------------
>>> Making hierarchy
--------------------------------------------------------------
cd /usr/src; make -f Makefile.inc1 hierarchy
...edited...
===> etc/sendmail (install)
cd /usr/src/etc/../share/man; make makedb
makewhatis /usr/share/man
makewhatis /usr/share/openssl/man
rm -rf /tmp/install.CQb9zEn9

freebsd7# mergemaster

*** The directory specified for the temporary root environment,
    /var/tmp/temproot, exists.  This can be a security risk if untrusted
    users have access to the system.

  Use 'd' to delete the old /var/tmp/temproot and continue
  Use 't' to select a new temporary root directory
  Use 'e' to exit mergemaster

  Default is to use /var/tmp/temproot as is

How should I deal with this? [Use the existing /var/tmp/temproot]
...edited...
--- /etc/motd   2009-08-21 13:55:29.000000000 -0400
+++ ./etc/motd  2009-08-21 20:23:59.000000000 -0400
@@ -1,4 +1,4 @@
-FreeBSD 7.1-RELEASE-p5 (FREEBSD7) #0: Fri Aug 21 12:59:27 EDT 2009
+FreeBSD ?.?.?  (UNKNOWN)

 Welcome to FreeBSD!
```

```
  Use 'd' to delete the temporary ./etc/motd
  Use 'i' to install the temporary ./etc/motd
  Use 'm' to merge the temporary and installed versions
  Use 'v' to view the diff results again

  Default is to leave the temporary file to deal with by hand

How should I deal with this? [Leave it for later] i
...edited...
 *** Temp ./COPYRIGHT and installed have the same CVS Id, deleting

*** Comparison complete
*** Saving mtree database for future upgrades

Do you wish to delete what is left of /var/tmp/temproot? [no]
 *** /var/tmp/temproot will remain

freebsd7# reboot
```

After rebooting, you see the new version of the FreeBSD kernel is installed (along with the userland).

```
freebsd7# uname -a
FreeBSD freebsd7.localdomain 7.1-RELEASE-p6 FreeBSD 7.1-RELEASE-p6 #1: Fri Aug 21 19:35:25 EDT 2009
root@freebsd7.localdomain:/usr/obj/usr/src/sys/FREEBSD7  i386
```

As you can see, Csup is functionally equivalent to CVSup, and Csup is packaged with the FreeBSD OS.

FreeBSD Update's Available Versions

In the first section of this paper, we saw FreeBSD Update used to keep a FreeBSD 7.2 system up-to-date. If you need to understand what sort of updates or upgrades are available for FreeBSD using freebsd-update, you can manually inspect one of the update sites. At the time of writing, visiting http://update2.freebsd.org displayed the following:

```
Index of /

         Name           Last Modified     Size        Type
   Parent Directory/                      -     Directory
   5.5-RELEASE/      2009-Jan-06 15:31:40 -     Directory
   6.0-RELEASE/      2009-Jan-06 15:31:40 -     Directory
   6.1-RELEASE/      2009-Jan-06 15:31:40 -     Directory
   6.2-RELEASE/      2009-Jan-06 15:31:40 -     Directory
   6.3-RELEASE/      2009-Jul-29 16:19:01 -     Directory
   6.4-RELEASE/      2009-Jul-29 16:19:09 -     Directory
   7.0-RELEASE/      2009-Apr-22 13:44:47 -     Directory
   7.1-BETA/         2009-Jan-06 15:31:40 -     Directory
   7.1-BETA2/        2009-Jan-06 15:31:40 -     Directory
   7.1-RC1/          2009-Jan-06 15:31:40 -     Directory
   7.1-RC2/          2009-Jan-07 20:16:13 -     Directory
   7.1-RELEASE/      2009-Jul-29 16:19:17 -     Directory
   7.2-BETA1/        2009-Apr-01 17:44:28 -     Directory
   7.2-RC1/          2009-Apr-22 14:00:51 -     Directory
   7.2-RC2/          2009-Apr-24 12:13:42 -     Directory
   7.2-RELEASE/      2009-Jul-29 16:19:26 -     Directory
   8.0-BETA1/        2009-Jul-30 06:04:42 -     Directory
   8.0-BETA2/        2009-Jul-30 06:04:51 -     Directory
   8.0-BETA3/        2009-Aug-23 21:25:58 -     Directory
   to-7.1-RELEASE/   2009-Jan-06 15:31:40 -     Directory
   to-7.2-BETA1/     2009-Apr-01 17:38:06 -     Directory
   to-7.2-RC1/       2009-Apr-16 15:20:25 -     Directory
   to-7.2-RC2/       2009-Apr-24 12:04:41 -     Directory
   to-7.2-RELEASE/   2009-May-02 17:45:12 -     Directory
   to-8.0-BETA1/     2009-Jul-08 01:06:26 -     Directory
   to-8.0-BETA2/     2009-Jul-17 19:08:49 -     Directory
   to-8.0-BETA3/     2009-Aug-23 22:04:57 -     Directory
   80BETA2.tar       2009-Jul-17 19:45:16 1.7G  application/x-tar
   80BETA3.tar       2009-Aug-23 22:38:23 1.5G  application/x-tar
   updates.tar       2009-Jul-30 06:32:07 13.9M application/x-tar
```

Take the 7.2-RELEASE/ directory as an example. This means that FreeBSD Upgrade knows how to start with FreeBSD 7.2 RELEASE (as we started the article) and update or upgrade to the "to-" directories. FreeBSD Update does not have the capability to update from 4.x, for example, or from any STABLE version (e.g., 7.2-STABLE).

For example, if you tried to use FreeBSD Upgrade to "update" a 7.2-STABLE system, it will fail:

```
fbsd71toS# uname -a
FreeBSD fbsd71toS.taosecurity.com 7.2-STABLE FreeBSD 7.2-STABLE #0: Sat Aug 22 23:02:30 EDT 2009
root@fbsd71toS.taosecurity.com:/usr/obj/usr/src/sys/FREEBSD7  i386

fbsd71toS# freebsd-update -v debug fetch
Looking up update.FreeBSD.org mirrors... 3 mirrors found.
Fetching public key from update5.FreeBSD.org... fetch: http://update5.FreeBSD.org/7.2-STABLE/i386/
pub.ssl: Not Found
failed.
```

If you are having trouble using FreeBSD Update, it's helpful to activate the '-v debug' switch to see what is happening.

FreeBSD Update to Upgrade from One Minor Version to Another

You've seen how CVSup and Csup can be used to update the OS and userland according to the tags in a supfile. You could easily continue this process if you wished to upgrade from FreeBSD 7.1 to FreeBSD 7.2 RELEASE. For example, your supfile would say the following:

```
*default host=INSERTYOURCHOICE.FreeBSD.org
*default base=/usr
*default prefix=/usr
*default release=cvs tag=RELENG_7_2_0
*default delete use-rel-suffix
*default compress
src-all
```

Notice we removed the date tag seen earlier. We also changed the release tag to indicate RELENG_7_2_0, which would be the same FreeBSD 7.2 shipped on CD.

It would make more sense to use RELENG_7_2 so the new system would be tracking the security branch.

It would be convenient if we could use binary upgrades via FreeBSD Update. It turns out that in this situation, we can do so. These are the basic commands:

```
freebsd-update upgrade -r 7.2-RELEASE
freebsd-update install
reboot
freebsd-update install
```

Note that this process requires plenty of free space in the /var partition. If you have more free space elsewhere (say in /usr), you can specific an alternative work directory for freebsd-update using the -d switch, e.g.,

```
freebsd-update -d /usr/db/freebsd-update upgrade -r 7.2-RELEASE
```

Ensure the specified directory exists before starting FreeBSD Update.

In the following example, we upgrade our FreeBSD 7.1 system to FreeBSD 7.2 using FreeBSD Update. FreeBSD Update will upgrade the system to the latest point in the security branch.

```
freebsd7# freebsd-update upgrade -r 7.2-RELEASE
Looking up update.FreeBSD.org mirrors... 3 mirrors found.
Fetching public key from update4.FreeBSD.org... done.
Fetching metadata signature for 7.1-RELEASE from update4.FreeBSD.org... done.
Fetching metadata index... done.
Fetching 2 metadata files... done.
Inspecting system... done.

The following components of FreeBSD seem to be installed:
kernel/generic src/base src/bin src/cddl src/contrib src/crypto src/etc
src/games src/gnu src/include src/krb5 src/lib src/libexec src/release
src/rescue src/sbin src/secure src/share src/sys src/tools src/ubin
src/usbin world/base world/dict world/doc world/games world/info
world/manpages world/proflibs

The following components of FreeBSD do not seem to be installed:
world/catpages

Does this look reasonable (y/n)? y

Fetching metadata signature for 7.2-RELEASE from update4.FreeBSD.org... done.
Fetching metadata index... done.
Fetching 1 metadata patches. done.
Applying metadata patches... done.
Fetching 1 metadata files... done.
Inspecting system... done.
Fetching files from 7.1-RELEASE for merging... done.
Preparing to download files... done.
Fetching 30039 patches.....10....20....30....40....50....60....70....80....90...
...edited...
..29390....29400....29410....29420....29430....29440....29450....29460....29470... done.
Applying patches... done.
Fetching 2273 files... done.
Attempting to automatically merge changes in files... done.

The following changes, which occurred between FreeBSD 7.1-RELEASE and
FreeBSD 7.2-RELEASE have been merged into /etc/group:
--- current version
+++ new version
@@ -1,6 +1,6 @@
-# $FreeBSD: src/etc/group,v 1.35.6.1 2008/11/25 02:59:29 kensmith Exp $
+# $FreeBSD: src/etc/group,v 1.35.8.1 2009/04/15 03:14:26 kensmith Exp $
 #
 wheel:*:0:root,analyst
 daemon:*:1:
 kmem:*:2:
 sys:*:3:
Does this look reasonable (y/n)? y

The following changes, which occurred between FreeBSD 7.1-RELEASE and
FreeBSD 7.2-RELEASE have been merged into /etc/master.passwd:
--- current version
+++ new version
@@ -1,6 +1,6 @@
-# $FreeBSD: src/etc/master.passwd,v 1.40.18.1 2008/11/25 02:59:29 kensmith Exp $
+# $FreeBSD: src/etc/master.passwd,v 1.40.20.1 2009/04/15 03:14:26 kensmith Exp $
 #
 root:$1$xvjnCDHU$FEOCCNdR1r99CTDQdtBWo0:0:0::0:0:Charlie &:/root:/bin/csh
 toor:*:0:0::0:0:Bourne-again Superuser:/root:
 daemon:*:1:1::0:0:Owner of many system processes:/root:/usr/sbin/nologin
 operator:*:2:5::0:0:System &:/:/usr/sbin/nologin
Does this look reasonable (y/n)? y

The following changes, which occurred between FreeBSD 7.1-RELEASE and
FreeBSD 7.2-RELEASE have been merged into /etc/passwd:
--- current version
+++ new version
@@ -1,6 +1,6 @@
-# $FreeBSD: src/etc/master.passwd,v 1.40.18.1 2008/11/25 02:59:29 kensmith Exp $
+# $FreeBSD: src/etc/master.passwd,v 1.40.20.1 2009/04/15 03:14:26 kensmith Exp $
```

```
 #
 root:*:0:0:Charlie &:/root:/bin/csh
 toor:*:0:0:Bourne-again Superuser:/root:
 daemon:*:1:1:Owner of many system processes:/root:/usr/sbin/nologin
 operator:*:2:5:System &:/:/usr/sbin/nologin
Does this look reasonable (y/n)? y

The following files will be removed as part of updating to 7.2-RELEASE-p3:
/boot/kernel/ath_hal.ko
...edited...
/usr/src/sys/vm/vm_pageq.c

The following files will be added as part of updating to 7.2-RELEASE-p3:
/boot/kernel/cpuctl.ko
...edited...
/usr/src/usr.sbin/makefs/walk.c

The following files will be updated as part of updating to 7.2-RELEASE-p3:
/.cshrc
/.profile
/COPYRIGHT
...edited...
/var/yp/Makefile.dist

freebsd7# freebsd-update install
Installing updates...
Kernel updates have been installed.  Please reboot and run
"/usr/sbin/freebsd-update install" again to finish installing updates.

freebsd7# reboot

freebsd7# freebsd-update install
Installing updates...done.

freebsd7# uname -a
FreeBSD freebsd7.localdomain 7.2-RELEASE-p2 FreeBSD 7.2-RELEASE-p2 #0: Wed Jun 24 00:57:44 UTC 2009
root@i386-builder.daemonology.net:/usr/obj/usr/src/sys/GENERIC  i386
```

As you can see, we used FreeBSD Update to bring our FreeBSD 7.1 system to the latest security update for FreeBSD 7.2. Notice we are running a GENERIC kernel again.

STABLE: The End of the Line for a Single Version

The end of the line in the FreeBSD 7.x tree is 7.2-STABLE. The STABLE tree incorporates not only bug fixes and security patches, but upgrades that are Merged From CURRENT (aka "MFC'd"). STABLE is a constantly moving target, marked only by the date and time that an administrator uses CVSup to sync with the STABLE tree. For this reason, security advisories, such as FreeBSD-SA-09:12.bind , will list the date and time at which a STABLE branch incorporates a security fix:

```
Corrected:      2009-07-28 23:59:22 UTC (RELENG_7, 7.2-STABLE)
```

If your STABLE is older than the date specified, your system is vulnerable. Compare that method of gauging a system's exposure to the "patch level" of running the security branch. From the same advisory:

```
                2009-07-29 00:14:14 UTC (RELENG_7_2, 7.2-RELEASE-p3)
```

Here we also have a timestamp, but it's easier to see that 7.2-RELEASE-p3 is patched for the bind vulnerability.

For demonstration purposes, we will upgrade our FreeBSD 7.2-RELEASE-p2 system to STABLE by modifying our supfile with these contents:

```
*default host=INSERTYOURCHOICE.FreeBSD.org
*default base=/usr
*default prefix=/usr
*default release=cvs tag=RELENG_7
```

```
*default delete use-rel-suffix
*default compress
src-all
```

```
check /usr/src/UPDATING
```

```
20090312:
        The open-source Atheros HAL has been merged from HEAD
        to STABLE.
        The kernel compile-time option AH_SUPPORT_AR5416 has been
        added to support certain newer Atheros parts, particularly
        PCI-Express chipsets.
        The following modules are no longer available, and should be
        removed from MODULES_OVERRIDE and/or loader.conf:-
         ath_hal ath_rate_amrr ath_rate_onoe ath_rate_sample
```

Next we follow the commands introduced earlier to upgrade to 7.2-STABLE. Begin with:

```
csup -g -L 2 /usr/local/etc/freebsd7-example.supfile
```

Then continue:

```
cp /usr/src/sys/i386/conf/GENERIC /usr/src/sys/i386/conf/FREEBSD7

cd /usr/src
make buildworld
make buildkernel KERNCONF=FREEBSD7
make installkernel KERNCONF=FREEBSD7

mergemaster -p
make installworld
mergemaster
reboot
```

When done you will be running FreeBSD 7.2-STABLE. When done our uname output appears as follows:

```
freebsd7# uname -a
FreeBSD freebsd7.localdomain 7.2-STABLE FreeBSD 7.2-STABLE #2: Sat Aug 22 17:12:42 EDT 2009
root@freebsd7.localdomain:/usr/obj/usr/src/sys/FREEBSD7  i386
```

Notice the output says 7.2-STABLE, although the CVS tag used was 7_RELENG.

Building a Userland and Kernel on One System and Installing on Another

In the following example, we will show how to install the userland and kernel built on one system onto a second system. The "server" with the desired userland and kernel is fbsd71toS, or 172.16.134.130.

```
fbsd71toS# uname -a
FreeBSD fbsd71toS.taosecurity.com 7.2-STABLE FreeBSD 7.2-STABLE #0: Sat Aug 22 23:02:30 EDT 2009
root@fbsd71toS.taosecurity.com:/usr/obj/usr/src/sys/FREEBSD7  i386
```

Since we are using NFS, the server has the following in /etc/rc.conf.

```
rpcbind_enable="YES"
nfs_server_enable="YES"
```

The server also has the following /etc/exports file.

```
fbsd71toS# cat /etc/exports
/usr    -alldirs
```

The "client" that will receive the new userland and kernel is freebsd7S.

```
freebsd7S# uname -a
FreeBSD freebsd7S.taosecurity.com 7.2-STABLE FreeBSD 7.2-STABLE #2: Sat Aug 22 17:12:42 EDT 2009
```

```
root@freebsd7.localdomain:/usr/obj/usr/src/sys/FREEBSD7  i386
```

The client has the following in /etc/rc.conf.

```
nfs_client_enable="YES"
```

First we mount /usr/src and /usr/obj from the server to the client using NFS.

```
freebsd7S# mount -t nfs 172.16.134.130:/usr/src /usr/src

freebsd7S# mount -t nfs 172.16.134.130:/usr/obj /usr/obj

freebsd7S# mount
/dev/ad0s1a on / (ufs, local)
devfs on /dev (devfs, local)
/dev/ad0s1f on /home (ufs, local, soft-updates)
/dev/ad0s1g on /tmp (ufs, local, soft-updates)
/dev/ad0s1d on /usr (ufs, local, soft-updates)
/dev/ad0s1e on /var (ufs, local, soft-updates)
172.16.134.130:/usr/src on /usr/src (nfs)
172.16.134.130:/usr/obj on /usr/obj (nfs)
```

Make sure we are now in /usr/src.

```
freebsd7S# cd /usr/src
```

At this point we can follow the instructions we saw earlier, starting as shown.

```
make installkernel KERNCONF=FREEBSD7

mergemaster -p
make installworld
mergemaster
```

Before reboot I umount the NFS mounts.

```
freebsd7S# pwd
/root
freebsd7S# umount /usr/ports
freebsd7S# umount /usr/src
freebsd7S# umount /usr/obj

reboot
```

When done we check the uname output on the client to see that it matches the server from whom it received its kernel and userland.

```
freebsd7S# uname -a
FreeBSD freebsd7S.taosecurity.com 7.2-STABLE FreeBSD 7.2-STABLE #0: Sat Aug 22 23:02:30 EDT 2009
root@fbsd71toS.taosecurity.com:/usr/obj/usr/src/sys/FREEBSD7  i386
```

That kernel matches the one on the server, so we just successfully installed a userland and kernel built on fbsd71toS onto a client, freebsd7.

What Comes Next?

Beyond STABLE comes CURRENT, or HEAD, or tag=. in a supfile. CURRENT represents the next version of FreeBSD. For example, while FreeBSD 7.x is the STABLE version, CURRENT is being prepared as FreeBSD 8.0. At the time of writing, FreeBSD 8.0 is currently in BETA. Although testing the next version of FreeBSD is encouraged in order to support the project and to ensure it works on your platforms, I do not recommened running CURRENT in production.

One could use CVSup or Csup to update to CURRENT using the following supfile:

```
*default host=INSERTYOURCHOICE.FreeBSD.org
*default base=/usr
```

```
*default prefix=/usr
*default release=cvs tag=.
*default delete use-rel-suffix
*default compress
src-all
```

However, when I want to try CURRENT, I prefer to start with a snapshot (http://www.freebsd.org/snapshots/) and either use the snapshot or CVSup to CURRENT from the snapshot. A snapshot is a version of FreeBSD from various branches. For example, at the time of writing, snapshots for FreeBSD 6.4-STABLE, 7.2-STABLE, and 8.0-CURRENT are posted.

Upgrading from One Major Version to Another Major Version Using FreeBSD Update

In the final example for this article, I will show how to use binary upgrades via FreeBSD update to upgrade from FreeBSD 7.1 RELEASE to FreeBSD 8.0 BETA3. I follow the instructions posted in the announcement for BETA3 (http://lists.freebsd.org/pipermail/freebsd-stable/2009-August/051628.html). By setting a proxy we can have the proxy provide copies of the updates to similar systems that might also need to perform the upgrade, as well as simply use a proxy to reach the Internet.

PLEASE NOTE that you should follow the instructions provided in any release announcement and not just those in this document. For example, the test system used in this article only has cmdwatch and screen installed. This is NOT typical of a production system. It is trivial for me to manually uninstall these applications compiled for 7.x and reinstall the latest versions compiled for 8.x. Therefore, I do not show those steps here.

The official documentation describes ways to handle applications installed as packages or using the ports tree.

This can take a long time, especially at the "Inspecting system... " stages.

```
fbsd71-to-8# uname -a
FreeBSD fbsd71-to-8.taosecurity.com 7.1-RELEASE FreeBSD 7.1-RELEASE #0: Thu Jan  1 14:37:25 UTC 2009
root@logan.cse.buffalo.edu:/usr/obj/usr/src/sys/GENERIC  i386

fbsd71-to-8# setenv HTTP_PROXY http://172.16.2.1:3128

fbsd71-to-8# freebsd-update upgrade -r 8.0-BETA3
Looking up update.FreeBSD.org mirrors... 3 mirrors found.
Fetching public key from update5.FreeBSD.org... done.
Fetching metadata signature for 7.1-RELEASE from update5.FreeBSD.org... done.
Fetching metadata index... done.
Fetching 2 metadata files... done.
Inspecting system... done.

The following components of FreeBSD seem to be installed:
kernel/generic world/base world/dict world/doc world/games world/info
world/manpages

The following components of FreeBSD do not seem to be installed:
src/base src/bin src/cddl src/contrib src/crypto src/etc src/games
src/gnu src/include src/krb5 src/lib src/libexec src/release src/rescue
src/sbin src/secure src/share src/sys src/tools src/ubin src/usbin
world/catpages world/proflibs

Does this look reasonable (y/n)? y

Fetching metadata signature for 8.0-BETA3 from update5.FreeBSD.org... done.
Fetching metadata index... done.
Fetching 1 metadata patches. done.
Applying metadata patches... done.
Fetching 1 metadata files... done.
Inspecting system...  done.
Fetching files from 7.1-RELEASE for merging... done.
Preparing to download files...
...edited...
9320....9330....9340....9350 done.
```

```
Applying patches...  done.
Fetching 750 files... done.
Attempting to automatically merge changes in files... done.

The following changes, which occurred between FreeBSD 7.1-RELEASE and
FreeBSD 8.0-BETA3 have been merged into /etc/group:
--- current version
+++ new version
@@ -1,6 +1,6 @@
-# $FreeBSD: src/etc/group,v 1.35.6.1 2008/11/25 02:59:29 kensmith Exp $
+# $FreeBSD: src/etc/group,v 1.35.10.1 2009/08/03 08:13:06 kensmith Exp $
 #
 wheel:*:0:root,analyst
 daemon:*:1:
 kmem:*:2:
 sys:*:3:
Does this look reasonable (y/n)? y

The following changes, which occurred between FreeBSD 7.1-RELEASE and
FreeBSD 8.0-BETA3 have been merged into /etc/master.passwd:
--- current version
+++ new version
@@ -1,6 +1,6 @@
-# $FreeBSD: src/etc/master.passwd,v 1.40.18.1 2008/11/25 02:59:29 kensmith Exp $
+# $FreeBSD: src/etc/master.passwd,v 1.40.22.1 2009/08/03 08:13:06 kensmith Exp $
 #
 root:$1$kF89UpDP$s8QA1LQcpsigLx9tQVgSa1:0:0::0:0:Charlie &:/root:/bin/csh
 toor:*:0:0::0:0:Bourne-again Superuser:/root:
 daemon:*:1:1::0:0:Owner of many system processes:/root:/usr/sbin/nologin
 operator:*:2:5::0:0:System &:/:/usr/sbin/nologin
Does this look reasonable (y/n)? y

The following changes, which occurred between FreeBSD 7.1-RELEASE and
FreeBSD 8.0-BETA3 have been merged into /etc/passwd:
--- current version
+++ new version
@@ -1,6 +1,6 @@
-# $FreeBSD: src/etc/master.passwd,v 1.40.18.1 2008/11/25 02:59:29 kensmith Exp $
+# $FreeBSD: src/etc/master.passwd,v 1.40.22.1 2009/08/03 08:13:06 kensmith Exp $
 #
 root:*:0:0:Charlie &:/root:/bin/csh
 toor:*:0:0:Bourne-again Superuser:/root:
 daemon:*:1:1:Owner of many system processes:/root:/usr/sbin/nologin
 operator:*:2:5:System &:/:/usr/sbin/nologin
Does this look reasonable (y/n)? y

The following files will be removed as part of updating to 8.0-BETA3-p0:
/boot/kernel/ath_hal.ko
/boot/kernel/ath_hal.ko.symbols
/boot/kernel/ath_rate.ko
...edited...
The following files will be added as part of updating to 8.0-BETA3-p0:
/boot/gptzfsboot
/boot/kernel/accf_dns.ko
...edited...
The following files will be updated as part of updating to 8.0-BETA3-p0:
/.cshrc
/.profile
/COPYRIGHT
...edited...
/var/named/etc/namedb/named.root
/var/yp/Makefile.dist

fbsd71-to-8# freebsd-update install
Installing updates...
Kernel updates have been installed.  Please reboot and run
"/usr/sbin/freebsd-update install" again to finish installing updates.
```

```
fbsd71-to-8# reboot

fbsd71-to-8# freebsd-update install
Installing updates...
Completing this upgrade requires removing old shared object files.
Please rebuild all installed 3rd party software (e.g., programs
installed from the ports tree) and then run "/usr/sbin/freebsd-update install"
again to finish installing updates.

fbsd71-to-8# pkg_info
cmdwatch-0.2.0_1    Watches the output from a command at specified intervals
screen-4.0.3_6      A multi-screen window manager
fbsd71-to-8# cd /var/db/pkg
fbsd71-to-8# pkg_delete cmdwatch-0.2.0_1/
fbsd71-to-8# pkg_delete screen-4.0.3_6/

fbsd71-to-8# reboot

fbsd71-to-8# uname -a
FreeBSD fbsd71-to-8.taosecurity.com 8.0-BETA3 FreeBSD 8.0-BETA3 #0: Sat Aug 22 02:36:50 UTC 2009
root@almeida.cse.buffalo.edu:/usr/obj/usr/src/sys/GENERIC  i386
```

That's it -- we're running FreeBSD 8.0 BETA3! We would have to reinstall our applications, which is covered in my related article on Keeping FreeBSD Applications Up-To-Date.

For reference, the 'install' prior to the first reboot installs the new kernel. The 'install' after the first reboot installs the new userland. The 'install' after the second reboot removes any old libraries used by applications that we removed (i.e., cmdwatch and screen).

Conclusion

I hope this article has helped you understand the different ways to keep a FreeBSD system up-to-date with security advisories. It is by no means comprehensive, but by following it you hopefully can judge the different ways to keep your system in sync with the latest security patches and fixes for FreeBSD.

Revision History
----

25 August 2009: Added material on building a userland and kernel on one system, plus upgrading major versions
24 August 2009: Minor fixes
23 August 2009: Additions regarding FreeBSD Update
22 August 2009: Draft FreeBSD 7.x version posted
21 April 2005: Minor typo corrections
24 December 2004: First publication