Security

FreeBSD Security Advisories

- http://www.freebsd.org/security/advisories.html

FreeBSD Security Advisories

This web page contains a list of released FreeBSD Security Advisories. See the FreeBSD Security Information page for general security information about FreeBSD.

Issues affecting the FreeBSD Ports Collection are covered in the FreeBSD VuXML document.

Date	Advisory name
2010-11-29	FreeBSD-SA-10:10.openssl
2010-11-10	FreeBSD-SA-10:09.pseudofs
2010-09-20	FreeBSD-SA-10:08.bzip2
2010-07-13	FreeBSD-SA-10:07.mbuf

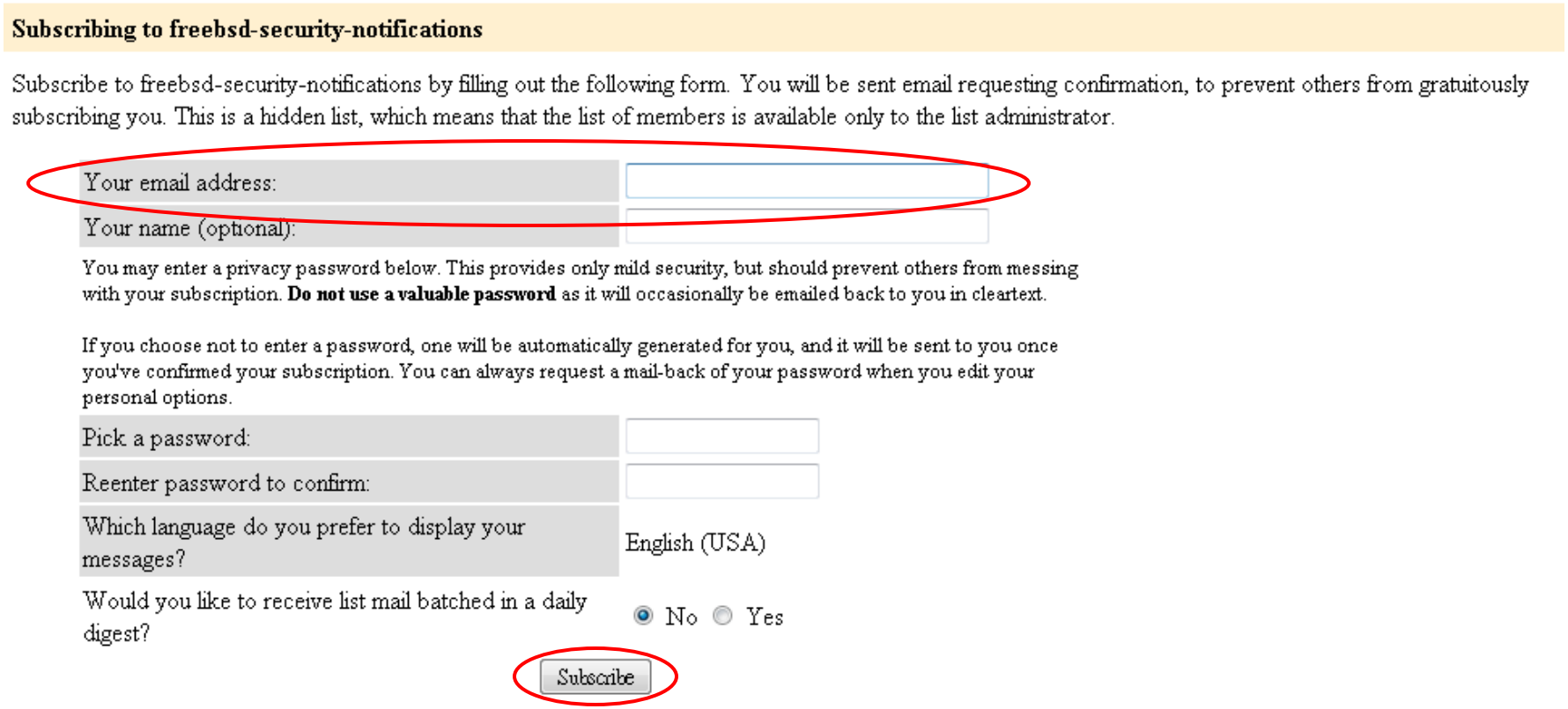
FreeBSD Security Advisories

- Advisory
  - Security information
- Where to find it
  - Web page (Security Advisories Channel)
    - http://www.freebsd.org

FreeBSD Security Advisories

❑ Where to find it

- freebsd-security-notifications Mailing list
  - ➢ http://lists.freebsd.org/mailman/listinfo/freebsd-security-notifications



Subscribing to freebsd-security-notifications

Subscribe to freebsd-security-notifications by filling out the following form. You will be sent email requesting confirmation, to prevent others from gratuitously subscribing you. This is a hidden list, which means that the list of members is available only to the list administrator.

Your email address:	
Your name (optional):	

You may enter a privacy password below. This provides only mild security, but should prevent others from messing with your subscription. **Do not use a valuable password** as it will occasionally be emailed back to you in cleartext.

If you choose not to enter a password, one will be automatically generated for you, and it will be sent to you once you've confirmed your subscription. You can always request a mail-back of your password when you edit your personal options.

Pick a password:	
Reenter password to confirm:	
Which language do you prefer to display your messages?	English (USA)
Would you like to receive list mail batched in a daily digest?	◉ No ○ Yes

Subscribe

FreeBSD Security Advisories

- Example
  - openssl

```
FreeBSD-SA-10:10.openssl                                  Security Advisory
                                                          The FreeBSD Project

Topic:          OpenSSL multiple vulnerabilities

Category:       contrib
Module:         openssl
Announced:      2010-11-29
Credits:        Georgi Guninski, Rob Hulswit
Affects:        FreeBSD 7.0 and later
Corrected:      2010-11-26 22:50:58 UTC (RELENG_8, 8.1-STABLE)
                2010-11-29 20:43:06 UTC (RELENG_8_1, 8.1-RELEASE-p2)
                2010-11-29 20:43:06 UTC (RELENG_8_0, 8.0-RELEASE-p6)
                2010-11-28 13:45:51 UTC (RELENG_7, 7.3-STABLE)
                2010-11-29 20:43:06 UTC (RELENG_7_3, 7.3-RELEASE-p4)
                2010-11-29 20:43:06 UTC (RELENG_7_1, 7.1-RELEASE-p16)
CVE Name:       CVE-2010-2939, CVE-2010-3864
```

FreeBSD Security Advisories

- CVE-2010-3864
  - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-3864

National Cyber-Alert System

Vulnerability Summary for CVE-2010-3864

Original release date: 11/17/2010

Last revised: 12/10/2010

Source: US-CERT/NIST

Overview

Multiple race conditions in ssl/t1_lib.c in OpenSSL 0.9.8f through 0.9.8o, 1.0.0, and 1.0.0a, when multi-threading and internal caching are enabled on a TLS server, might allow remote attackers to execute arbitrary code via client data that triggers a heap-based buffer overflow, related to (1) the TLS server name extension and (2) elliptic curve cryptography.

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 7.6 (HIGH) (AV:N/AC:H/Au:N/C:C/I:C/A:C) (legend)

Impact Subscore: 10.0

Exploitability Subscore: 4.9

FreeBSD Security Advisories

❑ Example

- Problem Description

```
I.   Background

FreeBSD includes software from the OpenSSL Project.  The OpenSSL Project is
a collaborative effort to develop a robust, commercial-grade, full-featured
Open Source toolkit implementing the Secure Sockets Layer (SSL v2/v3)
and Transport Layer Security (TLS v1) protocols as well as a full-strength
general purpose cryptography library.

II.  Problem Description

A race condition exists in the OpenSSL TLS server extension code
parsing when used in a multi-threaded application, which uses
OpenSSL's internal caching mechanism.  The race condition can lead to
a buffer overflow. [CVE-2010-3864]

A double free exists in the SSL client ECDH handling code, when
processing specially crafted public keys with invalid prime
numbers. [CVE-2010-2939]
```

FreeBSD Security Advisories

❑ Example

- Workaround

```
III. Impact

For affected server applications, an attacker may be able to utilize
the buffer overflow to crash the application or potentially run
arbitrary code with the privileges of the application. [CVE-2010-3864].

It may be possible to cause a DoS or potentially execute arbitrary in
the context of the user connection to a malicious SSL server.
[CVE-2010-2939]

IV.  Workaround

No workaround is available, but CVE-2010-3864 only affects FreeBSD 8.0
and later.

It should also be noted that CVE-2010-3864 affects neither the Apache
HTTP server nor Stunnel.
```

FreeBSD Security Advisories

- Example
  - Solution
    - Upgrade to
    - Source code patch
    - Binary patch

```
V.   Solution

Perform one of the following:

1) Upgrade your vulnerable system to 7-STABLE or 8-STABLE, or to the
RELENG_8_1, RELENG_8_0, RELENG_7_3, or RELENG_7_1 security branch
dated after the correction date.

2) To update your vulnerable system via a source code patch:

The following patches have been verified to apply to FreeBSD 7.1, 7.3,
8.0 and 8.1 systems.

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

[FreeBSD 7.x]
# fetch http://security.FreeBSD.org/patches/SA-10:10/openssl7.patch
# fetch http://security.FreeBSD.org/patches/SA-10:10/openssl7.patch.asc

[FreeBSD 8.x]
# fetch http://security.FreeBSD.org/patches/SA-10:10/openssl.patch
# fetch http://security.FreeBSD.org/patches/SA-10:10/openssl.patch.asc

b) Execute the following commands as root:

# cd /usr/src
# patch < /path/to/patch
# cd /usr/src/secure/lib/libssl
# make obj && make depend && make && 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>

3) To update your vulnerable system via a binary patch:

Systems running 7.1-RELEASE, 7.3-RELEASE, 8.0-RELEASE or 8.1-RELEASE
on the i386 or amd64 platforms can be updated via the
freebsd-update(8) utility:

# freebsd-update fetch
# freebsd-update install
```

Common Security Problems

- Software bugs
  - FreeBSD security advisor
  - portaudit (ports-mgmt/portaudit)
- Unreliable wetware
  - Phishing site
- Open doors
  - Account password
  - Disk share with the world

portaudit (1)

- portaudit
  - Checks installed ports against a list of security vulnerabilities
  - portaudit –Fda
    - -F: Fetch the current database from the FreeBSD servers.
    - -d: Print the creation date of the database.
    - -a: Print a vulnerability report for all installed packages.

- Security Output

portaudit (2)

- portaudit -Fda

```
auditfile.tbz                                 100% of   58 kB   38 kBps
New database installed.
Database created: Tue Nov 17 16:50:00 CST 2009
Affected package: libpurple-2.5.8
Type of problem: pidgin -- MSN overflow parsing SLP messages.
Reference: <http://portaudit.FreeBSD.org/59e7af2d-8db7-11de-883b-001e3300a30d.html>

Affected package: finch-2.5.8
Type of problem: pidgin -- MSN overflow parsing SLP messages.
Reference: <http://portaudit.FreeBSD.org/59e7af2d-8db7-11de-883b-001e3300a30d.html>

2 problem(s) in your installed packages found.

You are advised to update or deinstall the affected package(s) immediately.
```

- http://www.freshports.org/<category>/<portname>
  - http://www.freshports.org/databases/postgresql84-server/

portaudit (3)


FRESH ports
Port details
postgresql84-server 8.4.15_1 databases Σ=17
The most advanced open-source database available anywhere
Maintained by: pgsql@FreeBSD.org
Port Added: 07 Jul 2009 22:30:32
License: not specified in port
600 kW of N+1 redundant UPS power
THE NEW YORK INTERNET COMPANY
TEL: 800.288.7387 SITE: WWW.NYI.NET
PostgreSQL is a sophisticated Object-Relational DBMS, supporting
almost all SQL constructs, including subselects, transactions, and
user-defined types and functions. It is the most advanced open-source
database available anywhere. Commercial Support is also available.
The original Postgres code was the effort of many graduate students,

Common trick

- Tricks
  - ssh scan and hack
    - ssh guard
    - sshit
    - …
  - Phishing
  - XSS & sql injection
  - …
- Objective
  - Spam
  - Jump gateway
  - File sharing
  - …

Process file system - procfs

```
last pid:  8103;  load averages:  0.00,  0.03,  0.04
102 processes: 1 starting, 1 running, 100 sleeping
CPU states:  0.2% user,  0.0% nice,  1.7% system,  0.7% interrupt, 97.4% idle
Mem: 305M Active, 1402M Inact, 215M Wired, 81M Cache, 112M Buf, 3016K Free
Swap: 4096M Total, 352K Used, 4096M Free

  PID USERNAME   THR PRI NICE   SIZE    RES STATE  C   TIME   WCPU COMMAND
 4576 tyhsieh      1  76    0  1964K  1652K select 1  56:05  0.00% httpd
 4566 tyhsieh      1  76    0  1672K  1360K select 0   6:13  0.00% httpd
 4584 tyhsieh      1  76    0  1996K  1052K select 0   1:24  0.00% httpd
```

- Procfs
  - A view of the system process table
  - Normally mount on /proc
  - mount –t procfs proc /proc

```
hscc[/proc/4566] -chiahung- ls -al
total 0
dr-xr-xr-x  1 tyhsieh  hscc    0 Jan  3 13:53 ./
dr-xr-xr-x  1 root     wheel   0 Jan  3 13:53 ../
-r--r--r--  1 tyhsieh  hscc    0 Jan  3 13:53 cmdline
--w-------  1 tyhsieh  hscc    0 Jan  3 13:53 ctl
-r--r--r--  1 tyhsieh  hscc    0 Jan  3 13:53 etype
lr--r--r--  1 tyhsieh  hscc    0 Jan  3 13:53 file@ -> /home/tyhsieh/.etcdir/.etcvar/.etcexec/.etcvar/httpd
-r--r--r--  1 tyhsieh  hscc    0 Jan  3 13:53 map
-r--r--r--  1 tyhsieh  hscc    0 Jan  3 13:53 rlimit
-r--r--r--  1 tyhsieh  hscc    0 Jan  3 13:53 status
```

Simple SQL injection example

- User/pass authentication

```
SELECT * FROM usrTable
WHERE user =
AND pass = ;
```

- No input validation

```
SELECT * FROM usrTable
WHERE user = 'test'
AND pass = 'a' OR 'a' = 'a'
```

setuid program

- passwd

```
zfs[~] -chiahung- ls -al /usr/bin/passwd
-r-sr-xr-x  2 root  wheel  8224 Dec  5 22:00 /usr/bin/passwd
```

  - /etc/master.passwd is of mode 600 (-rw-------) !

- Setuid shell scripts are especially apt to cause security problems
  - Minimize the number of setuid programs

```
/usr/bin/find / -user root –perm -4000 –print |
/bin/mail –s “Setuid root files” username
```

  - Disable the setuid execution on individual filesystems
    - -o nosuid

Security issues

- /etc/hosts.equiv and ~/.rhosts
- Trusted remote host and user name DB
  - Allow user to login (via rlogin) and copy files (rcp) between machines without passwords
  - Format:
    - Simple: hostname [username]
    - Complex: [+-][hostname|@netgroup]
      [[+-][username|@netgorup]]
  - Example
    - bar.com foo (trust user "foo" from host "bar.com")
    - +@adm_cs_cc (trust all from amd_cs_cc group)
    - +@adm_cs_cc -@chwong
- Do not use this

Why not su nor sudo?

- Becoming other users
  - A pseudo-user for services, sometimes shared by multiple users

```
User_Alias newsTA=wangyr
Runas_Alias NEWSADM=news
newsTA  ALL=(NEWSADM) ALL
```

  - sudo –u news –s (?) Too dirty!
  - /etc/inetd.conf
    - login stream tcp nowait root /usr/libexec/rlogind rlogind
  - ~notftpadm/.rhosts
    - localhost wangyr
  - rlogin -l news localhost

Security tools

- nmap
- john, crack
- PGP
- CA
- …

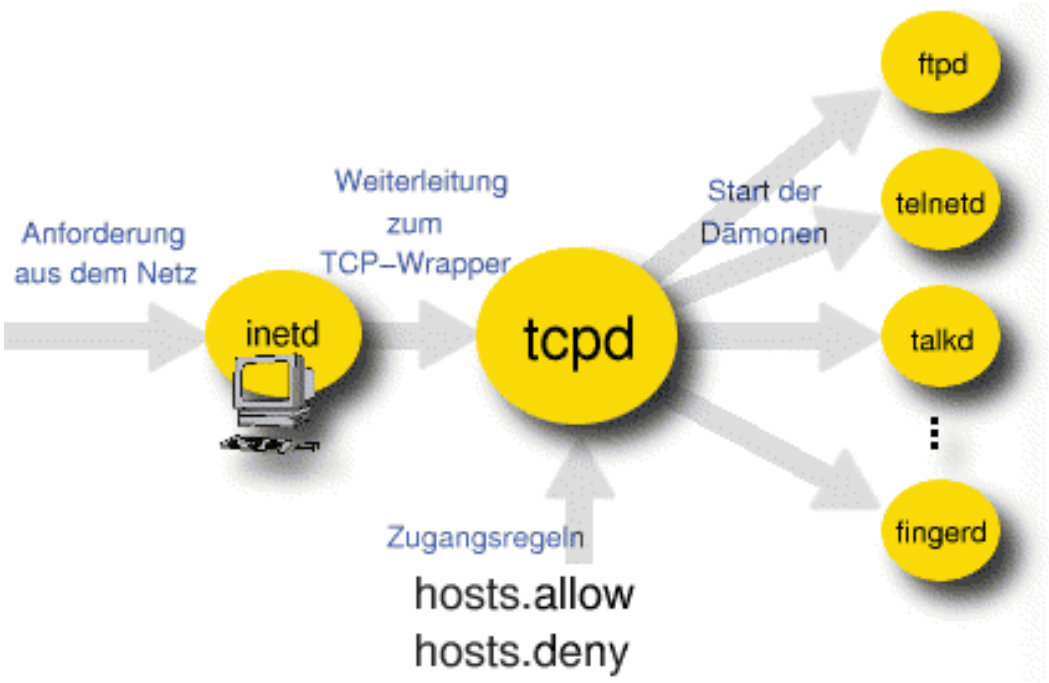
- Firewall
- TCP Wrapper
- …

TCP Wrapper

- There are something that a firewall will not handle
  - Sending text back to the source
- TCP wrapper
  - Extend the abilities of inetd
    - Provide support for every server daemon under its control
  - Logging support
  - Return message
  - Permit a daemon to only accept internal connetions

TCP Wrapper

- TCP Wrapper
  - Provide support for every server daemon under its control



TCP Wrapper

- To see what daemons are controlled by inetd, see /etc/inetd.conf

```
#ftp    stream  tcp     nowait  root    /usr/libexec/ftpd       ftpd -l
#ftp    stream  tcp6    nowait  root    /usr/libexec/ftpd       ftpd -l
#telnet stream  tcp     nowait  root    /usr/libexec/telnetd    telnetd
#telnet stream  tcp6    nowait  root    /usr/libexec/telnetd    telnetd
shell   stream  tcp     nowait  root    /usr/libexec/rshd       rshd
#shell  stream  tcp6    nowait  root    /usr/libexec/rshd       rshd
login   stream  tcp     nowait  root    /usr/libexec/rlogind    rlogind
#login  stream  tcp6    nowait  root    /usr/libexec/rlogind    rlogind
```

- TCP wrapper should not be considered a replacement of a good firewall. Instead, it should be used in conjunction with a firewall or other security tools

TCP Wrapper

- To use TCP wrapper
  1. inetd daemon must start up with "-Ww" option (default)
     Or edit /etc/rc.conf

```
inetd_enable="YES"
inetd_flags="-wW"
```

  - Edit /etc/hosts.allow
    - Format:
      daemon:address:action
      - daemon is the daemon name which inetd started
      - address can be hostname, IPv4 addr, IPv6 addr
      - action can be "allow" or "deny"
      - Keyword "ALL" can be used in daemon and address fields to means everything

/etc/hosts.allow

- First rule match semantic
  - Meaning that the configuration file is scanned in ascending order for a matching rule
  - When a match is found, the rule is applied and the search process will stop
- example

```
ALL :     localhost, loghost @adm_cc_cs : allow
ptelnetd pftpd sshd: @sun_cc_cs, @bsd_cc_cs, @linux_cc_cs : allow
ptelnetd pftpd sshd: zeiss, chbsd, sabsd : allow
identd :  ALL : allow
portmap :  140.113.17. ALL : allow
sendmail : ALL : allow
rpc.rstatd : @all_cc_cs 140.113.17.203: allow
rpc.rusersd : @all_cc_cs 140.113.17.203: allow
ALL : ALL : deny
```

/etc/hosts.allow

❑ Advance configuration

- External commands (twist option)
  - ➢ twist will be called to execute a shell command or script

```
# The rest of the daemons are protected.
telnet : ALL \
         : severity auth.info \
         : twist /bin/echo "You are not welcome to use %d from %h."
```

- External commands (spawn option)
  - ➢ spawn is like twist, but it will not send a reply back to the client

```
# We do not allow connections from example.com:
ALL : .example.com \
      : spawn (/bin/echo %a from %h attempted to access %d >> \
      /var/log/connections.log) \
      : deny
```

/etc/hosts.allow

- Wildcard (PARANOID option)
  - Match any connection that is made from an IP address that differs from its hostname

```
# Block possibly spoofed requests to sendmail:
sendmail : PARANOID : deny
```

❑ See

- man 5 hosts_access
- man 5 hosts_options

When you perform any change.

- Philosophy of SA
  - Know how things really work.
  - Plan it before you do it.
  - Make it reversible
  - Make changes incrementally.
  - Test before you unleash it .