Global Information Assurance Certification Paper

Building a secure DNS server and keeping it secure, using FreeBSD

Introduction

DNS and BIND and Vulnerabilities

The Domain Name System, or DNS, is one of the fundamental building blocks of the Internet. Without DNS we would not have the ability to translate numerical IP addresses into human-readable names, and the World Wide Web, as we know it, would likely not exist. The great majority of DNS servers run on some version of UNIX or Linux, and use the freely available Berkeley Internet Name Domain (BIND) daemon.

Unfortunately, BIND is not without its security flaws. According to CERT® (http://www.cert.org), "Since 1997, the CERT/CC has published twelve documents describing vulnerabilities or exploitation of vulnerabilities in BIND with information and advice on upgrading and preventing compromises. Unfortunately, many system and network administrators still have not upgraded their versions of BIND, making them susceptible to a number of vulnerabilities. Prior vulnerabilities in BIND have been widely exploited by intruders." (http://www.cert.org/advisories/CA-2001-02.html)

The Internet Software Consortium website (http://www.isc.org/products/BIND/bind-security.html) also lists the current vulnerabilities and bugs within different versions of BIND.

FreeBSD as a DNS Server

As a System Administrator tasked with creating a DNS solution for my company, one of my main concerns was the security of the system. My platform of choice for this server was FreeBSD; while it may not be any more or less secure than any other version of UNIX, I have had good success in building stable and reliable systems on FreeBSD, and have found FreeBSD to be exceptionally versatile and easy to configure.

FreeBSD is a mature operating system – FreeBSD 1.0 was released in 1993 – and is considered by many to be one of the most robust operating systems out there. For more information about the FreeBSD project, visit their website at http://www.freebsd.org.

This article will focus mostly on setting up and securing FreeBSD as a DNS server, but there will also be some references to overall OS hardening, since hardening the OS is a natural part of securing any service.

The version of FreeBSD covered in this article is 4.2-Release. On April 20, 2001, FreeBSD 4.3-Release was announced, which, among its many updates, included BIND version 8.3-Rel. However, there are some important points covered in this article that still apply to FreeBSD 4.3-Release.

BIND Vulnerabilities on FreeBSD

A search on the CERT® Coordination Center Advisories website (http://search.cert.org/) resulted in a recent advisory on multiple vulnerabilities in BIND:

> **Systems Affected**
>
> Domain Name System (DNS) Servers running various versions of ISC BIND (including both 4.9.x prior to 4.9.8 and 8.2.x prior to 8.2.3; 9.x is not affected) and derivatives. Because the normal operation of most services on the Internet depends on the proper operation of DNS servers, other services could be impacted if these vulnerabilities are exploited.

(http://www.cert.org/advisories/CA-2001-02.html)

Further reading on the above site shows two vulnerabilities that affect BIND version 8.2.x:

> **VU#196945 - ISC BIND 8 contains buffer overflow in transaction signature (TSIG) handling code**
>
> During the processing of a transaction signature (TSIG), BIND 8 checks for the presence of TSIGs that fail to include a valid key. If such a TSIG is found, BIND skips normal processing of the request and jumps directly to code designed to send an error response. Because the error-handling code initializes variables differently than in normal processing, it invalidates the assumptions that later function calls make about the size of the request buffer.

(http://www.cert.org/advisories/CA-2001-02.html)

and:

> **VU#325431 - Queries to ISC BIND servers may disclose environment variables**
>
> This vulnerability may allow attackers to read information from the program stack, possibly exposing environment variables. In addition, the information obtained by exploiting this vulnerability may aid in the development of exploits for VU#572183 and VU#868916.

(http://www.cert.org/advisories/CA-2001-02.html)

VU#196945 is quite serious. As explained in the "Impact" section of the advisory (below), it could allow an attacker to run commands on the server with the same privileges as the BIND daemon; in the case of a default installation of FreeBSD, BIND is run as root.

> **II. Impact**
>
> This vulnerability may allow an attacker to execute privileged commands or code with the same permissions as the BIND server. Because BIND is typically run by a superuser account, the execution would occur with superuser privileges.

(http://www.kb.cert.org/vuls/id/196945)

VU#325431 is also serious since it can help an attacker develop other exploits, although its immediate impact on the system is not be as severe as gaining root access. Again, this is explained in the Impact section of the CERT advisory:

> **II. Impact**
>
> This vulnerability may allow attackers to read information from the program stack, possibly exposing environment variables.

(http://www.kb.cert.org/vuls/id/325431)

The FreeBSD security website (http://www.freebsd.org/security) also has a security advisory posted, regarding the TSIG vulnerability:

```
=============================================================================
FreeBSD-SA-01:18                                          Security Advisory
                                                              FreeBSD, Inc.

Topic:          BIND remotely exploitable buffer overflow

Category:       core, ports
Module:         bind
Announced:      2001-01-31
Credits:        COVERT Labs <seclabs@NAI.COM>
                Claudio Musmarra
Affects:        All released versions of FreeBSD 3.x, 4.x.
                FreeBSD 3.5-STABLE prior to the correction date.
                FreeBSD 4.2-STABLE prior to the correction date.
                Ports collection prior to the correction date.
Corrected:      2001-01-30 (FreeBSD 3.5-STABLE)
                2001-01-29 (FreeBSD 4.2-STABLE)
                2001-01-29 (Ports collection)
Vendor status:      Updated version released
FreeBSD only:       NO

I.   Background

BIND is an implementation of the Domain Name Service (DNS) protocols.

II.  Problem Description
```

```
An overflowable buffer related to the processing of transaction
signatures (TSIG) exists in all versions of BIND prior to
8.2.3-RELEASE.  The vulnerability is exploitable regardless of
configuration options and affects both recursive and non-recursive DNS
servers.

Additional vulnerabilities allow the leaking of environment variables
and the contents of the program stack.  These vulnerabilities may
assist the ability of attackers to exploit the primary vulnerability
described above, and make provide additional information about the
state or configuration of the system.

All previous versions of BIND 8, such as the beta versions included in
FreeBSD 4.x prior to the correction date (designated the version
number BIND 8.2.3-T<#>B) are vulnerable to this problem.  Systems
running versions of BIND 9.x (available in the FreeBSD ports
collection) are unaffected.
. . .
```

(ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-01:18.bind.asc)

In a nutshell, what this advisory says is that 4.2-Release does in fact contain this vulnerability, and that the vulnerability is corrected in 4.2-STABLE or greater, as well as in the updated Ports collection.

Since there is at least one known exploit for this vulnerability (an example is located on the Security Focus website at: http://www.securityfocus.com/data/vulnerabilities/exploits/tsig.c), it is vital that you check whether your system is vulnerable, and patch it accordingly.

How to check if you are vulnerable

The FreeBSD security advisory above explains that all versions of BIND 8 prior to BIND 8.2.3-RELEASE are vulnerable, and it gives some good quick instructions to check whether you are running a vulnerable version of BIND:

```
To check whether a DNS server is running a vulnerable version of BIND,
perform the following command as any user:

% dig @serverip version.bind. CHAOS TXT

The following segment of output indicates a non-vulnerable server running
BIND 8.2.3-RELEASE:

...
;; ANSWER SECTION:
VERSION.BIND.           0S CHAOS TXT    "8.2.3-REL"
...
```

(ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-01:18.bind.asc)

What's the solution?

There are several solutions offered in the FreeBSD advisory including: upgrading the Ports collection and installing BIND 8 from ports; downloading and installing an unofficial tarball; and some instructions for a partial workaround; however the preferred method in this case is to upgrade to the STABLE release of FreeBSD.

```
V.   Solution
. . .

[Base system]

Upgrade your vulnerable FreeBSD system to 3.5-STABLE or 4.2-
STABLE after the respective correction dates.
```

(ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-01:18.bind.asc)

By upgrading the OS to the –STABLE branch, you not only patch the BIND vulnerability, but you get the benefit of installing the latest bug fixes since the latest release.

To find out more about FreeBSD-STABLE, read section 19.2.2. Staying Stable with FreeBSD of the FreeBSD Handbook at:
http://www.freebsd.org/doc/en_US.ISO_8859-1/books/handbook/current-stable.html

Installation Options

You can save yourself a lot of work, especially when it comes to securing the system, by installing FreeBSD from scratch. FreeBSD offers several different methods of installation, including FTP over the Internet, downloading and burning an installation CD image, or by purchasing a CD. Whichever method you choose, be sure that your source is a valid, trusted source. The FreeBSD website (http://www.freebsd.org) maintains a list of official mirror sites for downloads, as well as links to resellers who sell official FreeBSD CD sets (e.g. the Walnut Creek CD-Rom site at http://www.osd.bsdi.com/).
If you can't install from scratch, make certain that you are aware of every service running on your system and verify that there are no known vulnerabilities in them. You will need to upgrade the system to the latest STABLE release in order to patch the BIND vulnerabilities. This is explained further in the section "Upgrading to FreeBSD-STABLE" later in this document.

Installing from CD

Installing FreeBSD from CD is the quickest method, and if you have purchased a copy of the CD then it is the best method for ensuring that your source is trusted.

The downside to installing from CD is that FreeBSD doesn't release the STABLE version on CD (STABLE is a daily snapshot of bug and security fixes) so you will need to upgrade to STABLE after you have installed from CD.

If you do choose to install from CD, the website "FreeBSD Cheat Sheets" http://www.mostgraveconcern.com/freebsd/install.html) by author Dan O'Connor contains some excellent step-by-step instructions, which I highly recommend as a reference along with the FreeBSD Handbook instructions. (http://www.freebsd.org/doc/en_US.ISO_8859-1/books/handbook/install.html).

Upgrading to FreeBSD-STABLE

Once you have installed the OS (or if you are working with an existing install of the OS), you will need to upgrade your system to STABLE in order to patch the BIND security hole as well as any other FreeBSD patches. The FreeBSD Handbook has some instructions on upgrading to STABLE (http://www.freebsd.org/doc/en_US.ISO_8859-1/books/handbook/current-stable.html), however the "FreeBSD Cheat Sheets" site offers a much more detailed set of instructions at: http://www.mostgraveconcern.com/freebsd/cvsup.html

Installing FreeBSD-STABLE from Scratch Via the Internet.
If you decide to install via the Internet, you can install the latest STABLE release directly, simply by downloading the latest boot floppies from the STABLE branch, and running the installation. There is an excellent article by Marty Schlacter entitled "How to Build a FreeBSD-STABLE Firewall with IPFILTER" (http://www.schlacter.dyndns.org/public/FreeBSD-STABLE_and_IPFILTER.html), which gives extremely detailed instructions on installing FreeBSD-STABLE from scratch. Aside from the fact that you will probably not want to set up your DNS server as a firewall / gateway, Mr. Schlacter's article is very comprehensive and applies quite well to any FreeBSD server set-up.

Some Installation Tips

Whichever method you choose to install the OS, there are a few tips you can follow to help ensure your system is as secure as possible from the outset, and save yourself some work later on.

1. Plan on installing the DNS server behind a firewall, and allow only TCP and UDP ports 53 through the firewall. While a firewall is by no means the only solution, a good perimeter defence is one of the keys to successful network security.
2. Ensure you have enough disk space to install the necessary distribution. At least 2GB is recommended.

3. When selecting which distribution to install, choose option #4 – "Developer" to install full sources, binaries and docs, but no games.
4. Choose "yes" to install the ports collection.
5. Do not install the XWindow system. It is not needed for a DNS server, and it may expose you to other vulnerabilities.
6. Do not install any other packages unless absolutely needed. There should be no need for a web browser, mail reader, etc. on a DNS server. All that you need is already included in the base system, including SSH for remote access.
7. Select "Yes" when asked if this machine will be a leaf node (i.e. not a gateway)
8. Select "only normal users to access FTP". This will disable Anonymous FTP (later on you will disable FTP altogether).
9. Select "No" to NFS server and NFS client.
10. When prompted for a Default Security profile, select "Extreme". This will shut down inetd and various other services. It's better to start off with these services closed, and open them as needed.
    According to the Help file in the install,

```
Extreme security settings have been selected.

This means that all "popular" network services and mechanisms like
inetd(8) have been DISABLED by default.  PLEASE NOTE that this
still does not save you from having to properly secure your system
in other ways or exercise due diligence in your administration,
this simply picks a more secure set of out-of-box defaults to
start with.

To change any of these settings later, edit /etc/rc.conf
```

    (FreeBSD 4.2-RELEASE Installation Help File, May 15, 2001)

11. Do not install Linux Binary support – again, it's not needed for a DNS server, and not only can it potentially open up any possible vulnerabilities (such as the "Lion Worm") that exist on Linux systems, the majority of applications that run on Linux have already been ported to run natively on FreeBSD.
12. Choose a strong root password, and plan on changing it often.

Securing the DNS Server

Now that you have a STABLE system up and running, there are a few things to be done to ensure that your DNS server is as secure as possible.

First of all, you will need to ensure that the upgrade has in fact upgraded BIND to a "secure" version. Run the command:

```
# dig @123.123.123.123 version.bind. CHAOS TXT
```

(where "123.123.123.123" is your server's IP address). You should now see the following output:

```
; <<>> DiG 8.3 <<>> @123.123.123.123 version.bind. CHAOS TXT
; (1 server found)
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUERY SECTION:
;;      version.bind, type = TXT, class = CHAOS

;; ANSWER SECTION:
VERSION.BIND.           0S CHAOS TXT    "8.2.3-REL"
```

The last line of the output tells us that the BIND version is now 8.2.3-REL, which, according to the FreeBSD Security Advisory, is not open to the TSIG and environment variable vulnerabilities.

Another way to help protect your system is to mask the version so that if anyone runs the above command, they will not (easily) be able to tell what version of BIND you are running. You can do this in FreeBSD simply by editing the file /etc/namedb/named.conf and adding the line:

```
version "XXX";
```

into the "options" section of the file. (You can customize the text within the quotes to suit your own tastes). This will cause the output of the dig command to appear as follows:

```
# dig @123.123.123.123 version.bind. CHAOS TXT

; <<>> DiG 8.3 <<>> @123.123.123.123 version.bind. CHAOS TXT
; (1 server found)
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUERY SECTION:
;;      version.bind, type = TXT, class = CHAOS

;; ANSWER SECTION:
VERSION.BIND.           0S CHAOS TXT    "XXX"
```

As you can see, the version reported is "XXX". This is a weak defence at best; however anything you can do to thwart an attack can only help in overall system security. If you do change this option, remember to keep a record of what version of BIND you are actually running, in the very likely case that another vulnerability is discovered. For more information about the named.conf file syntax, consult the named.conf man page.

You will also want to run the name daemon as an unprivileged user, so that when another vulnerability is discovered, the impact will be reduced on your server until you can patch it. The FreeBSD security advisory gives the following instructions on how to run named as an unprivileged user:

```
Add the following line to /etc/rc.conf:

named_flags="-u bind -g bind"  # Flags for named

Add the following line to your /etc/namedb/named.conf file, in
the
"options" section:

      pid-file "/var/named/named.pid";

See the named.conf(5) manual page for more details about
configuring
named.

Perform the following commands as root:

Create a directory writable by the bind user where named can
store its
pid file:

# mkdir /var/named
# chown bind:bind /var/named

Shut down the DNS server:

# ndc stop

Restart it using the non-privileged user and group:

# ndc -p /var/named/named.pid start -u bind -g bind
```

(ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-01:18.bind.asc)

You should also edit /etc/rc.conf as follows so that named will always run as the non-privileged user at system startup:

```
named_enable="YES"
named_flags="-u bind -g bind"  # Flags for named
```

Now that the above steps are done, you can now be assured that your DNS server is no longer vulnerable to the TSIG or environment variable vulnerabilities, and it will be difficult to cause undue harm via the name daemon.

What to Do Next

Your job is by no means over. As an administrator of a system attached to the Internet, you will need to be vigilant and watch for any new vulnerabilities, as well

as monitor your system for any attempted attacks. Subscribe to various security newsletters such as SANS, CERT, and FreeBSD-Security. Tracking the websites for bulletins and updates is also a good plan to keep on top of security issues.

Monitor the BIND website (http://www.isc.org/products/BIND) for any updates to BIND and in particular monitor the security portion of the site (http://www.isc.org/products/BIND/bind-security.html).

If possible, set up an intrusion detection system on your DNS server – a popular one is Snort (http://www.snort.org) , which can be installed via FreeBSD ports. Installing Tripwire (http://www.tripwire.org) can also be a huge help in monitoring your system for any changes or unusual activity. You can also set up packet filtering (firewall) software on FreeBSD. FreeBSD comes with two popular packet filtering packages: IPFW and IPFILTER. Either one makes an excellent firewall. Remember to investigate any bugs or vulnerabilities in any package you decide to install.

Schedule regular upgrades to FreeBSD-STABLE. Once a month should be more than sufficient to keep your system up-to-date. Anything more frequent may cause more downtime than you will be prepared to handle.

Finally, remember that any good Unix security practices also apply to FreeBSD, so it is a good idea to learn as much as possible about Unix security and apply this knowledge to your FreeBSD server.

Sources:

CERT® Coordination Center
http://www.cert.org
24 May, 2001

CERT® Advisory CA-2001-02 Multiple Vulnerabilities in BIND
http://www.cert.org/advisories/CA-2001-02.html
10 May, 2001

CERT® Vulnerability Note VU#196945
"ISC BIND 8 contains buffer overflow in transaction signature (TSIG) handling code"
http://www.kb.cert.org/vuls/id/196945
May 2001

CERT® Vulnerability Note VU#325431
"Queries to ISC BIND servers may disclose environment variables"
http://www.kb.cert.org/vuls/id/325431
May 2001

CERT® Vulnerability Note VU#572183
"ISC BIND 4 contains buffer overflow in nslookupComplain()"
http://www.kb.cert.org/vuls/id/572183
May 2001

CERT® Vulnerability Note VU#868916
"ISC BIND 4 contains input validation error in nslookupComplain()"
http://www.kb.cert.org/vuls/id/868916
May 2001

CERT® Coordination Center Search Engine
http://search.cert.org
28 May, 2001

Internet Software Consortium – BIND
http://www.isc.org/products/BIND
25 May, 2001

Internet Software Consortium: BIND Vulnerabilities
http://www.isc.org/products/BIND/bind-security.html
May 2001

The FreeBSD Project
http://www.freebsd.org

25 May, 2001

FreeBSD Security Information
http://www.freebsd.org/security
05 May, 2001

FreeBSD Handbook – Chapter 19.2: "-CURRENT vs. –STABLE"
http://www.freebsd.org/doc/en_US.ISO_8859-1/books/handbook/current-stable.html
January 2001

FreeBSD Handbook – Chapter 2: "Installing FreeBSD"
http://www.freebsd.org/doc/en_US.ISO_8859-1/books/handbook/install.html
January 2001

FreeBSD Security Advisory FreeBSD-SA-01:18
ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-01:18.bind.asc
31 January, 2001

FreeBSD 4.2-RELEASE Installation Help File
15 May, 2001

FreeBSD File Formats Manual – named.conf(5)
7 January, 1999

Dan O'Connor, "FreeBSD Cheat Sheets"
http://www.mostgraveconcern.com/freebsd/
01 January, 2001

Dan O'Connor, "Installing FreeBSD"
http://www.mostgraveconcern.com/freebsd/install.html
10 May, 2001

Dan O'Connor, "Updating Sources with CVSUP"
http://www.mostgraveconcern.com/freebsd/cvsup.html
01 January, 2001

Marty Schlacter, "How to Build a FreeBSD-STABLE Firewall with IPFILTER"
http://www.schlacter.dyndns.org/public/FreeBSD-STABLE_and_IPFILTER.html
28 May, 2001

Security Focus
http://www.securityfocus.com
28 May, 2001

Security Focus – "ISC Bind 8 Transaction Signatures Buffer Overflow Vulnerability"
http://www.securityfocus.com/bid/2302

"lame named 8.2.x remote exploit"
by lx (adresadeforward@yahoo.com) and lucysoft (lucysoft@hotmail.com)
http://www.securityfocus.com/data/vulnerabilities/exploits/tsig.c
28 May, 2001

Windriver – "The Walnut Creek CDROM Collection"
http://www.osd.bsdi.com/
4 April, 2001

Snort – the Open Source Network Intrusion Detection System
http://www.snort.org
22 May, 2001

The Tripwire Open Source Project
http://www.tripwire.org
28 May, 2001