The FreeBSD Security Officer function

BSDCan, 19 May 2007

Simon L. Nielsen
FreeBSD Deputy Security Officer
http://people.FreeBSD.org/~simon/

FreeBSD®

Overview

- FreeBSD *quick* intro
- FreeBSD security handling
- Keep yourself up-to-date
- ”Case study”

FreeBSD *quick* introduction

- Base system
  - CURRENT, -STABLE, -RELEASE branches
- Ports Collection
- Committers have CVS access
- Core team, elected ”political” leaders

Security Team organization

(May 2007)

Security Officer
Colin Percival

Security Officer Team (so@)
Jacques Vidrine, Simon L. Nielsen,
Robert Watson

Security Team (secteam@)
Marcus Alves Grando, Remko Lodder,
George V. Neville-Neil, Philip Paeps,
Christian S.J. Peron, Dag-Erling C. Smørgrav

Authority

- Security Officer chosen by the old Security Officer
- Security Officer approved by Core team
- Security Officer vets Security Team

Security Officer Charter

- Keeping the community informed of bugs, exploits, popular attacks, and other risks.
- Acting as a liaison on behalf of the FreeBSD Project with external organizations regarding sensitive, non-public security issues.
- Monitoring the appropriate channels for reports of bugs, exploits, and other circumstances that may affect the security of a FreeBSD system.
- ... http://security.FreeBSD.org/charter.html

Handling of security issues

- Evaluation of severity
- Warn FreeBSD.org Admins Team, if needed
- Contact domain experts
- Create / test bugfix (patch)
- Coordinate within FreeBSD (re, portmgr)
- Prepare security advisory
- Coordinate with other vendors
- Commit fix and send out advisory

Finding out about issues

- Public resources
  - Bugtraq, full-disclosure
  - Secunia
  - FreeBSD mailing lists, GNATS
- Private
  - secteam@, security-officer@
- Vendor coordination
  - vendor-sec, US-CERT, CPNI (was NISCC)

Supported FreeBSD versions

- Normal support – 1 year
- Extended support – 2 years
- 5.5, 5-STABLE (EoL May 31, 2008)
- 6.1, 6.2, 6-STABLE (EoL May 31, 2008...)

Vulnerability types

- Remote code execution
- Remote denial of service (DoS)
- Local privilege escalation
- Local denial of service

Security Advisory

FreeBSD-SA-07:03.ipv6 Security Advisory
The FreeBSD Project

Topic: IPv6 Routing Header 0 is dangerous

Category: core
Module: ipv6
Announced: 2007-04-26
Credits: Philippe Biondi, Arnaud Ebalard, Jun-ichiro itojun Hagino
Affects: All FreeBSD releases.
Corrected: 2007-04-24 11:42:42 UTC (RELENG_6, 6.2-STABLE)
2007-04-26 23:42:23 UTC (RELENG_6_2, 6.2-RELEASE-p4)
2007-04-26 23:41:59 UTC (RELENG_6_1, 6.1-RELEASE-p16)
2007-04-24 11:44:23 UTC (RELENG_5, 5.5-STABLE)
2007-04-26 23:41:27 UTC (RELENG_5_5, 5.5-RELEASE-p12)
CVE Name: CVE-2007-2242

I. Background

IPv6 provides a routing header option which allows a packet sender to indicate how the packet should be routed, overriding the routing knowledge present in a network. This functionality is roughly equivalent to the "source routing" option in IPv4. All nodes in an IPv6 network -- both routers and hosts -- are required by RFC 2460 to process such headers.

Security Advisory...

II. Problem Description

There is no mechanism for preventing IPv6 routing headers from being used to route packets over the same link(s) many times.

III. Impact

An attacker can "amplify" a denial of service attack against a link between
two vulnerable hosts; that is, by sending a small volume of traffic the attacker can consume a much larger amount of bandwidth between the two vulnerable hosts.

An attacker can use vulnerable hosts to "concentrate" a denial of service attack against a victim host or network; that is, a set of packets sent over a period of 30 seconds or more could be constructed such that they all arrive at the victim within a period of 1 second or less.

Other attacks may also be possible.

Security Advisory...

```
V.   Solution

NOTE WELL: The solution described below causes IPv6 type 0 routing headers
to be ignored.  Support for IPv6 type 0 routing headers can be re-enabled
if required by setting the newly added net.inet6.ip6.rthdr0_allowed sysctl
to a non-zero value.

Perform one of the following:

1) Upgrade your vulnerable system to 5-STABLE, or 6-STABLE, or to the
RELENG_6_2, RELENG_6_1, or RELENG_5_5 security branch dated after the
correction date.

...
```

Security Advisory...

```
...

2) To patch your present system:

The following patches have been verified to apply to FreeBSD 5.5, 6.1,
and 6.2 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-07:03/ipv6.patch
# fetch http://security.FreeBSD.org/patches/SA-07:03/ipv6.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.
```

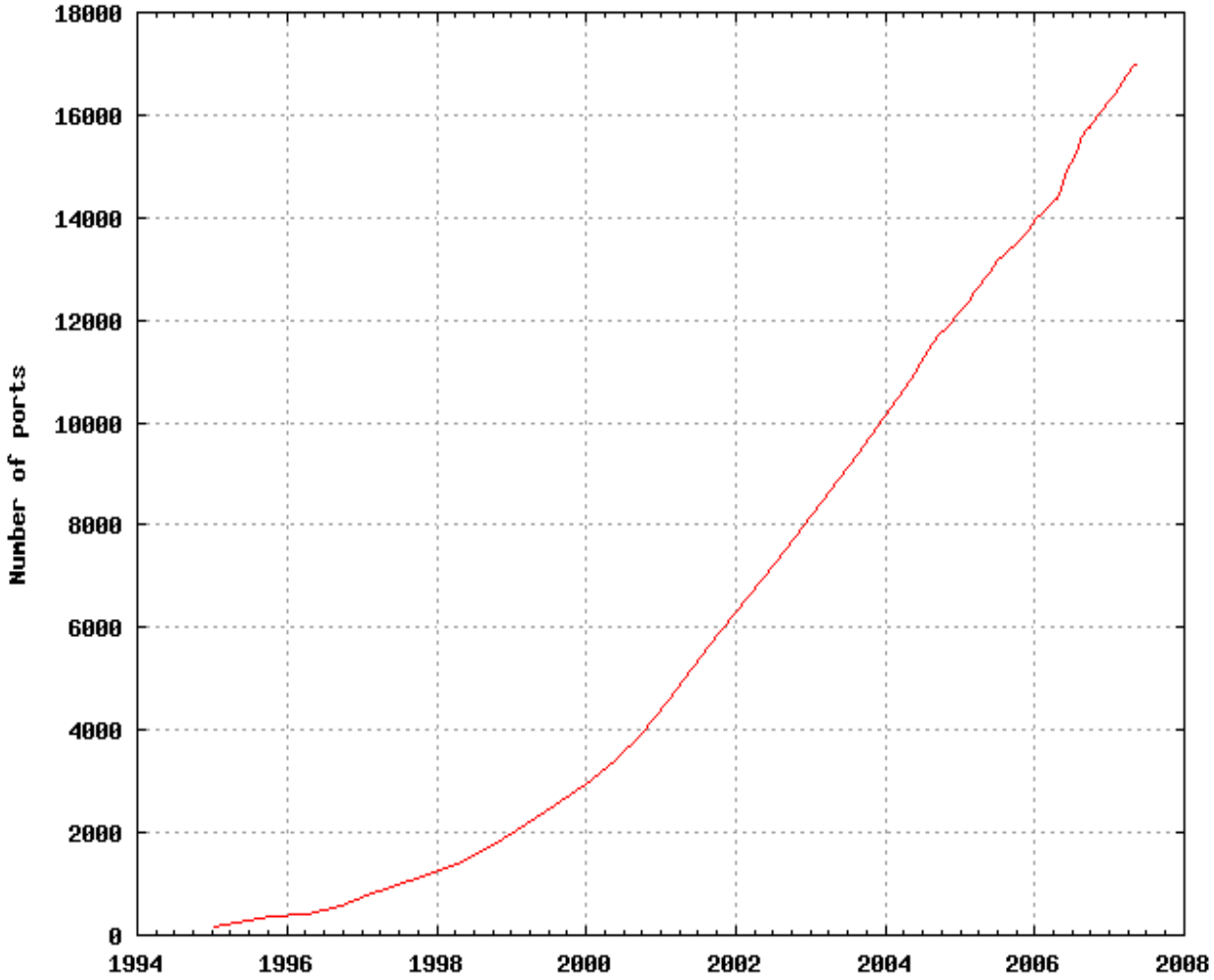
Security Advisory...

```
VI.  Correction details

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

Branch                                                          Revision
  Path
- -------------------------------------------------------------------------
RELENG_5
  src/sys/netinet6/in6.h                                          1.35.2.5
  src/sys/netinet6/in6_proto.c                                    1.29.2.5
  src/sys/netinet6/route6.c                                       1.10.4.2
RELENG_5_5
  src/UPDATING                                               1.342.2.35.2.12
  src/sys/conf/newvers.sh                                     1.62.2.21.2.14
  src/sys/netinet6/in6.h                                        1.35.2.3.2.1
  src/sys/netinet6/in6_proto.c                                  1.29.2.4.2.1
  src/sys/netinet6/route6.c                                     1.10.4.1.4.1

...
```

Security Advisory...

```
VII. References

http://www.secdev.org/conf/IPv6_RH_security-csw07.pdf

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2242

The latest revision of this advisory is available at
http://security.FreeBSD.org/advisories/FreeBSD-SA-07:03.ipv6.asc

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.6 (FreeBSD)

iD8DBQFGM8/CFdaIBMps37IRAu30AJ9nDSBQetafO6QPf8pJSA7Fwk6qlQCePVg0
2T4oPjAuyPYX9bkmP0EAdfs=
=MGTg
-----END PGP SIGNATURE-----
```

FreeBSD Ports Collection



http://www.FreeBSD.org/ports/growth/status.png

Ports Collection security

- Almost 17.000 ports
- Security advisory
- Security notes
- VuXML (Vulnerability and eXposure Markup Language)
- Maintainer normally fixes ports
- Maintainer bypass

VuXML example

```
<vuln vid="dc8c08c7-1e7c-11db-88cf-000c6ec775d9">
 <topic>apache -- mod_rewrite buffer overflow vulnerability</topic>
 <affects>
  <package>
   <name>apache</name>
   <range><ge>1.3.28</ge><lt>1.3.36_1</lt></range>
   <range><ge>2.0.46</ge><lt>2.0.58_2</lt></range>
   <range><ge>2.2.0</ge><lt>2.2.2_1</lt></range>
  </package>
 </affects>
 <description>
  <body xmlns="http://www.w3.org/1999/xhtml">
   <p>The Apache Software Foundation and The Apache HTTP Server
    Project reports:</p>
   <blockquote cite="http://marc.theaimsgroup.com/?l=apache-httpd-
  announce&amp;m=115409818602955">
     <p>An off-by-one flaw exists in the Rewrite module,
      mod_rewrite, as shipped with Apache 1.3 since 1.3.28, 2.0
      since 2.0.46, and 2.2 since 2.2.0.</p>
...
```

VuXML example...

```
...
    <p>The Apache HTTP Server project thanks Mark Dowd of McAfee
     Avert Labs for the responsible reporting of this
     vulnerability.</p>
   </blockquote>
  </body>
 </description>
 <references>
  <certvu>395412</certvu>
  <cvename>CVE-2006-3747</cvename>
  <mlist
  msgid="44CA22D9.6020200@apache.org">http://marc.theaimsgroup.com/?l=apac
  he-httpd-announce&amp;m=115409818602955</mlist>
 </references>
 <dates>
  <discovery>2006-07-27</discovery>
  <entry>2006-07-28</entry>
 </dates>
</vuln>
```

VuXML.org web site

FreeBSD VuXML

Documenting security issues in FreeBSD and the FreeBSD Ports Collection

Security issues that affect the FreeBSD operating system or applications in the FreeBSD Ports Collection are documented using the **Vulnerabilities and Exposures Markup Language (*VuXML*)**. The current VuXML document that serves as the source for the content of this site can be found:

- in the FreeBSD Ports Collection repository, path ports/security/vuxml/vuln.xml
- as a local copy
- as a local copy, compressed with bzip2

Please report security issues to the FreeBSD Security Team at <security-team@FreeBSD.org>. Full contact details, including information handling policies and PGP key, can be found on the FreeBSD Security page.

entry date index

by package name	by topic	by CVE name	by entry date	by modified date	by VuXML ID

Entered	Topic
2006-08-17	horde -- Phishing and Cross-Site Scripting Vulnerabilities
2006-08-15	globus -- Multiple tmpfile races
2006-08-13	alsaplayer -- multiple vulnerabilities
	mysql -- format string vulnerability
	postgresql -- encoding based SQL injection

VuXML.org web site

x11vnc -- authentication bypass vulnerability

FreeBSD VuXML: Documenting security issues in FreeBSD and the FreeBSD Ports Collection

Affected packages
x11vnc < 0.8.2

Details

VuXML ID	9dda3ff1-2b02-11db-a6e2-000e0c2e438a
Discovery	2006-08-08
Entry	2006-08-13

Ludwig Nussel reports that x11vnc is vulnerable to an authentication bypass vulnerability. The vulnerability is caused by an error in auth.c. This could allow a remote attacker to gain unauthorized and unauthenticated access to the system.

References

Bugtraq ID	18977
CVE Name	CVE-2006-2450
URL	http://bugs.debian.org/376824

portaudit

```
$ portaudit -a
Affected package: cacti-0.8.6g_41
Type of problem: cacti -- ADOdb "server.php" Insecure Test Script
Security Issue.
Reference: <http://www.FreeBSD.org/ports/portaudit/79c1154d-d5a5-
11da-8098-00123ffe8333.html>

Affected package: ghostscript-gnu-7.07_13
Type of problem: ghostscript -- insecure temporary file creation
vulnerability.
Reference: <http://www.FreeBSD.org/ports/portaudit/27a70a01-5f6c-
11da-8d54-000cf18bbe54.html>

2 problem(s) in your installed packages found.

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

Other jobs

- Maintenance of secteam systems
- Portsnap
- freebsd-update

Keep yourself up-to-date

- Subscribe to freebsd-announce
- Portaudit
- freebsd-update
- Bugtraq, full-disclosure, Secunia

rc.d/jail race - SA-07:01.jail

- 2006-12-21 – Initial report
- 2006-12-29 – re@ poked
- 2007-01-01 – First draft patch
- 2007-01-07 – cperciva ”breaks” patch
- 2007-01-11 – Advisory released
- 2007-01-15 – FreeBSD 6.2 released

Apache - CVE-2006-3747

- 2006-07-25 NISCC
- 2006-07-25 Fix FreeBSD.org systems
- 2006-07-25 vendor-sec
- 2006-07-27 Advise port maintainers...
- 2006-07-27 Fix committed

Patch CVE-2006-3747

```
--- src/modules/standard/mod_rewrite.c   (revision 421288)
+++ src/modules/standard/mod_rewrite.c   (working copy)
@@ -2736,7 +2736,7 @@
              int c = 0;

              token[0] = cp = ap_pstrdup(p, cp);
-             while (*cp && c < 5) {
+             while (*cp && c < 4) {
                  if (*cp == '?') {
                      token[++c] = cp + 1;
                      *cp = '\0';
```

The End