FreeBSD Security Officer funktionen

BSD-DK, 26 August 2006

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

FreeBSD®

FreeBSD introduction

- BSD nedarvet open source operativsystem
- Base system
  - CURRENT/STABLE ”branches”
- Ports Collection
- Committers har adgang til CVS
- Core team, valgt ”politisk” ledelse

Security Team organisering

(August 2006)

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

Autoritet

- Security Officer valgt af tidligere Security Officer
- Security Officer accepteret af Core
- Security Officer vælger 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

Håndtering af sikkerheds issues

- Orientering om problem
- Evaluering af alvorlighed
- Adviser evt. FreeBSD.org Admins Team
- Evt. kontakt af ”ekspert”
- Test / lav fejlrettelse (patch)
- Forbered security advisory
- Koordiner med andre vendors
- ”Commit” fix og send advisory ud

Orientering om problem

- Offentligt
  - Bugtraq, full-disclosure
  - Secunia
  - FreeBSD post lister, GNATS
- Privat
  - secteam@, so@
- Vendor koordinering
  - vendor-sec, US-CERT, NISCC

Understøttede versioner

- Normal support – 1 år
- Udvidet support – 2 år
- 4.11, 4-STABLE (EoL January 31, 2007)
- 5.3, 5.4, 5.5, 5-STABLE (EoL May 31, 2008)
- 6.0, 6.1, 6-STABLE (EoL May 31, 2008...)

Sårbarheds type

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

Security Advisory

```
FreeBSD-SA-06:17.sendmail                                  Security Advisory
                                                         The FreeBSD Project

Topic:          Incorrect multipart message handling in Sendmail

Category:       contrib
Module:         contrib_sendmail
Announced:      2006-06-14
Affects:        All FreeBSD releases.
Corrected:      2006-06-14 15:58:23 UTC (RELENG_6, 6.1-STABLE)
                2006-06-14 15:59:28 UTC (RELENG_6_1, 6.1-RELEASE-p2)
                2006-06-14 15:59:37 UTC (RELENG_6_0, 6.0-RELEASE-p9)
                2006-06-14 16:00:02 UTC (RELENG_5, 5.5-STABLE)
                2006-06-14 16:00:22 UTC (RELENG_5_5, 5.5-RELEASE-p2)
                2006-06-14 16:00:42 UTC (RELENG_5_4, 5.4-RELEASE-p16)
                2006-06-14 16:00:56 UTC (RELENG_5_3, 5.3-RELEASE-p31)
                2006-06-14 16:01:06 UTC (RELENG_4, 4.11-STABLE)
                2006-06-14 16:01:21 UTC (RELENG_4_11, 4.11-RELEASE-p19)
CVE Name:       CVE-2006-1173
```

Security Advisory...

I. Background

FreeBSD includes sendmail(8), a general purpose internetwork mail routing facility, as the default Mail Transfer Agent (MTA).

II. Problem Description

A suitably malformed multipart MIME message can cause sendmail to exceed predefined limits on its stack usage.

III. Impact

An attacker able to send mail to, or via, a server can cause queued messages on the system to not be delivered, by causing the sendmail process which handles queued messages to crash. Note that this will not stop new messages from entering the queue (either from local processes, or incoming via SMTP).

IV. Workaround

No workaround is available, but systems which do not receive email from untrusted sources are not vulnerable.

Security Advisory...

```
V.   Solution

Perform one of the following:

1) Upgrade your vulnerable system to 4-STABLE, 5-STABLE, or 6-STABLE,
or to the RELENG_6_1, RELENG_6_0, RELENG_5_5, RELENG_5_4, RELENG_5_3,
or RELENG_4_11 security branch dated after the correction date.

2) To patch your present system:

The following patches have been verified to apply to FreeBSD 4.11, 5.3,
5.4, 5.5, 6.0, and 6.1 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-06:17/sendmail.patch
# fetch http://security.FreeBSD.org/patches/SA-06:17/sendmail.patch.asc

b) Execute the following commands as root:

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

Security Advisory...

```
VI.  Correction details

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

Branch                                                          Revision
  Path
-
-------------------------------------------------------------------------
RELENG_4
  src/contrib/sendmail/src/deliver.c                          1.1.1.3.2.24
  src/contrib/sendmail/src/mime.c                             1.1.1.3.2.14
  src/contrib/sendmail/src/sendmail.h                         1.1.1.4.2.31
RELENG_4_11
  src/UPDATING                                              1.73.2.91.2.19
  src/sys/conf/newvers.sh                                   1.44.2.39.2.22
  src/contrib/sendmail/src/deliver.c                      1.1.1.3.2.17.2.2
  src/contrib/sendmail/src/mime.c                          1.1.1.3.2.8.2.2
  src/contrib/sendmail/src/sendmail.h                     1.1.1.4.2.19.2.2
...
```

Security Advisory...

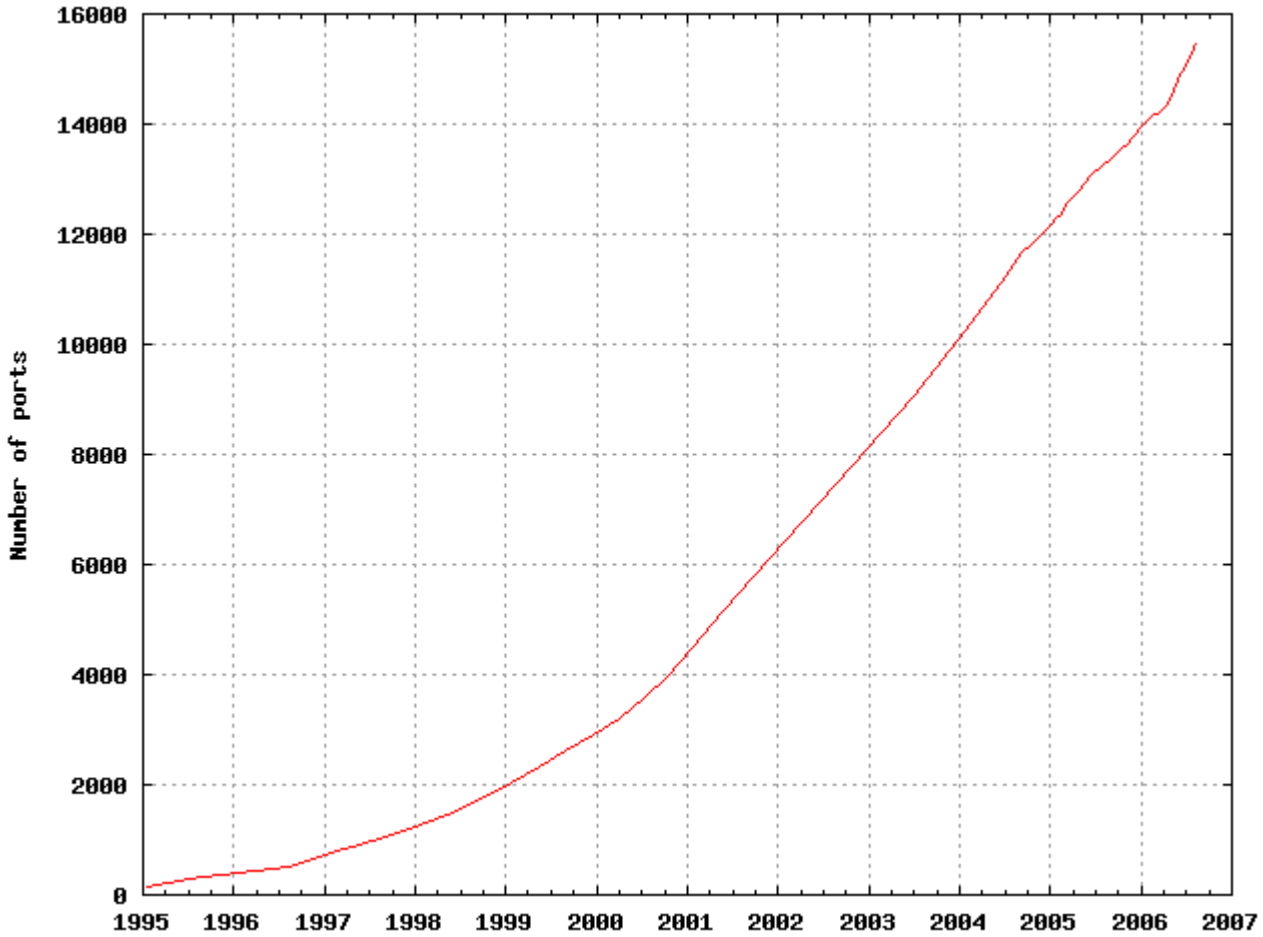
```
VII. References

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1173

The latest revision of this advisory is available at
http://security.FreeBSD.org/advisories/FreeBSD-SA-06:17.sendmail.asc
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.3 (FreeBSD)

iD8DBQFEkDVJFdaIBMps37IRAqUCAJwKg8UZ2a5oO9XLXpPwgsBi+YdQcACgj2IY
D5jN+o1IfjomEK4IIY+xiR8=
=t7Wz
-----END PGP SIGNATURE-----
```

FreeBSD Ports Collection



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

Ports Collection sikkerhed

- Ca. 15.500 ports
- Security advisory
- Security notes
- VuXML (Vulnerability and eXposure Markup Language)
- ”Maintainer” retter normalt ports
- Maintainer bypass

VuXML eksempel

```
<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 eksempel

```
...
    <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=ap
  ache-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.
```

Hold dig opdateret

- Tilmeld -announce
- Portaudit
- freebsd-update
- Bugtraq, full-disclosure, Secunia

Apache - CVE-2006-3747

- 07-25 NISCC
- 07-25 Fix FreeBSD.org systemer
- 07-25 vendor-sec
- 07-27 Adviser port maintainers...
- 07-27 Fix committet

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