```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

                NetBSD Security Advisory 2015-008
                =================================

Topic:          OpenSSL and TLS protocol vulnerabilities


Version:        NetBSD-current:         source prior to July 7th
                NetBSD 6.1 - 6.1.5:     affected
                NetBSD 6.0 - 6.0.6:     affected
                NetBSD 5.1 - 5.1.4:     affected
                NetBSD 5.2 - 5.2.2:     affected
                pkgsrc:                 affected

Severity:       remote DoS, confidentiality compromise

Fixed:          NetBSD-current:         Jul 7th, 2015
                NetBSD-7 branch:        Jul 11th, 2015
                NetBSD-6-0 branch:      Jul 12th, 2015
                NetBSD-6-1 branch:      Jul 12th, 2015
                NetBSD-6 branch:        Jul 12th, 2015
                NetBSD-5-2 branch:      Aug 14th, 2015
                NetBSD-5-1 branch:      Aug 14th, 2015
                NetBSD-5 branch:        Aug 14th, 2015
                pkgsrc:                 openssl-1.0.2d corrects these issues

Teeny versions released later than the fix date will contain the fix.

Please note that NetBSD releases prior to 5.1 are no longer supported.
It is recommended that all users upgrade to a supported release.


Abstract
========

This advisory covers the OpenSSL Security Advisory of June 11th, 2015
which lists seven different vulnerabilities that affect NetBSD releases;
also, the OpenSSL Security Advisory of July 9th, 2015 with one vulnerability
that affected only NetBSD-current:

DHE man-in-the-middle protection (Logjam, CVE-2015-4000)
Malformed ECParameters causes infinite loop (CVE-2015-1788)
Exploitable out-of-bounds read in X509_cmp_time (CVE-2015-1789)
PKCS7 crash with missing EnvelopedContent (CVE-2015-1790)
CMS verify infinite loop with unknown hash function (CVE-2015-1792)
Race condition handling NewSessionTicket (CVE-2015-1791)
Invalid free in DTLS (CVE-2014-8176)

and
Alternative chains certificate forgery (CVE-2015-1793)

Also, in NetBSD 5 a regression was introduced October 19th last year
concerning the SSL server code.


Technical Details
=================

See https://www.openssl.org/news/secadv/20150611.txt
and https://www.openssl.org/news/secadv/20150709.txt

The regression in NetBSD 5.* was due to a faulty application
```

```
of the POODLE mitigation code, and made the SSL server fail
the client handshake request, with the exception of SSLv3
and TLS1 handshakes where RC4_MD5 was an acceptable cipher,
which would then be the cipher getting used.
In summary this caused a comparably weak cipher to be used
if the connection succeeded as all.

Fixing this problem provides only limited help, though:
Please be aware that while the crypto library from the OpenSSL in
NetBSD 5.x is still ok, that is not true for the ssl library.
The ssl library supports as newest and safest protocol TLS 1.0,
and that is no longer considered good enough. At the same time
we cannot just update OpenSSL on that branch to a newer version
since all available newer ones are incompatible.


Solutions and Workarounds
=========================

Solution:
Update the OpenSSL libraries and restart all affected services.

Users of NetBSD 5.*:
Please consider using OpenSSL from pkgsrc for all uses where you
actually want secure SSL connections.
Programs in that use libssl are: amd, pkgtools, postfix, hostapd,
wpa_supplicant, httpd and the ldap client.
In cases where you use the encrypted communications feature of
these programs across an untrusted medium, using replacements
from pkgsrc is recommended as well.


- From source:
+-----------
Update src and rebuild and install.

For NetBSD-6*, NetBSD-7* and NetBSD-current:
cvs update -dP -r <branch> crypto/external/bsd/openssl

- From tarballs:
+-------------
To obtain fixed binaries, fetch the appropriate base.tgz and comp.tgz
from a daily build later than the fix dates, from
http://nyftp.netbsd.org/pub/NetBSD-daily/<rel>/<date>/<arch>/binary/sets/
with a date later than the fix date for your branch as listed above,
and your release version and architecture
(e.g. http://nyftp.netbsd.org/pub/NetBSD-daily/netbsd-6-1/201503XXXX00Z/amd64/binary/sets/),
and then extract the files:

Shared libraries:

tar xzpf base.tgz \*libssl\* \*libcrypto\*

And static libraries and linker config files:

tar xzpf comp.tgz \*libssl\* \*libcrypto\*

Get the fixed library into use
+----------------------------
Since the vulnerability is in a shared library, getting the old
library purged and the fixed one into use requires restarting
all programs that load libssl.
The easiest way to do this is to reboot the system.

Another method, using /bin/sh:
```

```
ps ax -o pid | (while read pid; do \
        pmap $pid | egrep '(libssl|libcrypto)' && echo found $pid ;\
done)

will find non-chrooted programs that have the affected libraries open;
you'll need to restart them.
sshd, ntp and named may not show up in this list since they may
run chrooted and re-exec'ed but they also would need to be restarted.
ldd <programname> will show the shared libraries a program will
want to use.


Thanks To
=========

Thanks to the OpenSSL development team for the advisory and fixes.
OpenSSL also credits:
Joseph Birr-Pixton for reporting CVE-2015-1788
Robert Swiecki (Google) and Hanno BÃ¶ck for reporting CVE-2015-1789
Michal Zalewski (Google) for reporting CVE-2015-1790
Johannes Bauer for reporting CVE-2015-1792
Praveen Kariyanahalli, Ivan Fratric (Google) and Felix Groebert (Google)
        for reporting CVE-2014-8176
Adam Langley (Google/BoringSSL), David Benjamin (Google/BoringSSL) for
        reporting CVE-2015-1793

Revision History
================

        2015-08-19      Initial release


More Information
================

Advisories may be updated as new information becomes available.
The most recent version of this advisory (PGP signed) can be found at
  http://ftp.NetBSD.org/pub/NetBSD/security/advisories/NetBSD-SA2015-008.txt.asc

Information about NetBSD and NetBSD security can be found at
http://www.NetBSD.org/ and http://www.NetBSD.org/Security/ .


Copyright 2015, The NetBSD Foundation, Inc.  All Rights Reserved.
Redistribution permitted only in full, unmodified form.

$NetBSD: NetBSD-SA2015-008.txt,v 1.1 2015/08/19 18:15:33 tonnerre Exp $

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v2

iQIcBAEBCAAGBQJV1NmoAAoJEAZJc6xMSnBuZ9YP/jnYE8sOgl5xRlZ+VkDdKwOX
qNlbU9yJHV2rDX3OV35jiR7dkcbF0itg9ZCqIEi+v3Shnv9WwEHE4y5miPUwb6fp
tPL77MIvPx0J3fshVQYgg27jMJWekQZLGSxC4wO2iYKWxKlZsVjsoiTtosJw9Toe
kPh7VVjK5u2I/DfISSHuzm6pLMkuudZxm5DuUN3KcQnvd6i4MPPlEEo1D8nT39hr
bSycxfRHk0wKxI/Yw5RmNprgjM2BQUig89abvFd+7RqnXE3rRiAM86g64L4LmcxH
o1IoSzGqWJ8gaqVcZqJLEt7Za4oe0O8cD108m5BaftHmOTUNA4ecVABtyJyRqDxs
jv03MCVZm1CH9qIG8mMKb+N+f4xHyLNzD8XwrMFBrUl2WSh8n+6RSK1r4XVMIW2+
YJb1z6/GHp7LId5Fv2fDrLGLEY0TVP9ts5tNOEqCkzozPe4zuWI4PeowXFqqdBnq
BBiP0uKz/uGFS9XoRO/a28EuOgMrzZhegzsvraZBzXyDiPrGH2B21aysWci5W/nG
mqcnTHUnQRtWnKBfJQj9hy9Zqm+O6ZyRe/Q9jwgStpMHksxbJETl49dX2TqOMBG7
M/hqpz10ddUO/0PEOeDiDLK/eH7qQrTdY03zB2z/iB6DNqBqzziRsvTGYIIoI3MF
JUFxcYt5UFrwsjQpDtks
```

```
=068Q
-----END PGP SIGNATURE-----
```