Heartbleed
The Live Action Monologue

Just over 40 slides / April 23rd, 2014
Cruft to Content ratio ~1:3

Rights of pictures per copyright holder/creator
OpenSSL 1.0.1
Standard Disclaimer

- My own opinion and views, not that of anyone else (most especially not my employer)
- I’m sorry in advance for whatever I may have done
- I’m sorry for whatever I did in the past
- I didn’t mean it that way (unless that way is correct and good)
- Go make your own informed decisions
“Looking for a talking head...”
OpenSSL = ...

... an open-source implementation of the SSL and TLS protocols
What’s a Heartbeat?

“A HeartbeatRequest message can arrive almost at any time during the lifetime of a connection. Whenever a HeartbeatRequest message is received, it SHOULD be answered with a corresponding HeartbeatResponse message.” - RFC 6520

Ben Sapiro (CC-BY-SA), 2014
CVE-2014-0160

OpenSSL version 1.01(A-E)
/* Enter response type, length and copy payload */
*bp++ = TLS1_HB_RESPONSE;
s2n(payload, bp);
memcpy(bp, pl, payload);

User controlled
What is not

- It is not a virus
- It is not a flaw in SSL or TLS
- It is not a flaw in any cipher suite
- It does not affect all web sites
- Does not directly impact other software outside of OpenSSL/LibSSL
- It is not an issue with all versions of OpenSSL
- It is not a BoF, ROP or any other voodoo
XKCD explains

HOW THE HEARTBLEED BUG WORKS:

1. User Meg wants these 6 letters: POTATO. User
2. Server, are you still there? If so, reply "POTATO" (6 LETTERS).
3. User Meg wants these 6 letters: POTATO. User
4. Server, are you still there? If so, reply "POTATO" (6 LETTERS).

Ben Sapiro (CC-BY-SA), 2014
XKCD explains

SERVER, ARE YOU STILL THERE? IF SO, REPLY "BIRD" (4 LETTERS).

User Olivia from London wants pages about "man in car why". Note: Files for IP 375.381.283.17 are in /tmp/files-3843. User Meg wants these 4 letters: BIRD. There are currently 340 connections open. User Brendan uploaded the file following (contents: 834be62a25eb9ff91v3k6f8)

HMM...

User Olivia from London wants pages about "man in car why". Note: Files for IP 375.381.283.17 are in /tmp/files-3843. User Meg wants these 4 letters: BIRD. There are currently 340 connections open. User Brendan uploaded the file following (contents: 834be62a25eb9ff91v3k6f8)
XKCD explains

SERVER, ARE YOU STILL THERE? IF SO, REPLY "HAT" (500 LETTERS).

User Meg wants these 500 letters: HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about snakes but not too long. User Karen wants to change account password to "ColHe1t".
At least two discoverers of 2 year old vulnerability

@neelmehta of Google Security

Ben Sapiro (CC-BY-SA), 2014
A logo & semi-responsible disclosure

The Heartbleed Bug

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).

The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.
What’s at risk of exposure

- usernames and passwords
- cookie values
- user provided data = {credit card numbers, private information, email addresses}
- encryption keys (maybe)
  … anything that can be sent to a web server
  … anything in process memory that includes LibSSL/OpenSSL
<table>
<thead>
<tr>
<th>Frame (1159 bytes)</th>
<th>Decrypted SSL record (1040 bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000 02 03 fd 68 65 61 72 74 62 6c 65 64 6e 61 6d 69</td>
<td>...heartbleed.fi</td>
</tr>
<tr>
<td>0010 6c 69 70 70 6f 2e 69 6f 59 45 4c 4f 46 57 20 53</td>
<td>lippo.ioYELLOW S</td>
</tr>
<tr>
<td>0020 44 2d 49 42 5f 00 00 00 00 00 00 00 00 00 00 00</td>
<td>UBMARINE'......=.</td>
</tr>
</tbody>
</table>
| 0030 6e 74 69 6d 65 72 62 71 75 67 70 79 | -Agent: Mozilla/
| 0040 6d 65 6e 61 6d 65 20 73 6f 75 73 74 61 74 | Intel Mac OS X 1
| 0050 70 72 6f 6e 65 61 6c 6c 69 73 6f 72 69 6e 67 | 0_9_2) AppleWebKit
| 0060 65 78 74 65 6e 61 6d 65 63 61 6c 73 74 69 6e 67 | it/537.36 (KHTML,
| 0070 78 2c 69 6e 66 6f 72 20 6d 65 73 69 74 69 63 6c | like Gecko) Ch
| 0080 69 6e 66 6f 72 6d 65 6e 61 6d 65 67 6f 6f 70 | rome/33.0.1750.1
| 0090 6e 61 6d 65 63 61 6c 73 74 69 6e 67 20 73 65 6c | 52 Safari/537.36
| 00a0 73 74 65 73 73 69 6e 67 65 6e 61 6d 65 72 69 6e | .Referer: https
| 00b0 73 65 63 6f 6e 66 69 6c 65 6d 65 69 6e 67 74 6f | /cs-screenshot.
| 00c0 63 6f 6e 64 69 66 69 6e 67 74 6f 6c 65 6d 65 | .lan/captures.A
| 00d0 66 69 6c 65 6d 65 63 61 6c 73 74 69 6e 67 74 | ccept-Encoding:
| 00e0 6f 66 20 74 69 6d 65 6d 69 6e 67 74 6f 6c 65 | gzip, deflate, sdc
| 00f0 6c 65 61 76 65 6c 6f 6e 65 72 69 6e 67 74 6f | h. Accept-Langua
| 0100 6e 61 6d 65 63 61 6c 73 74 69 6e 67 74 6f 6c 65 | ge: en-US, en;q=0
| 0110 66 69 6c 65 6d 65 63 61 6c 73 74 69 6e 67 74 6f | .8..Cookie: _ses
| 0120 65 6e 63 65 73 74 61 74 69 6e 67 74 6f 6c 65 | sion_id=df5c5d87
| 0130 63 6f 6e 64 69 66 69 6e 67 74 6f 6c 65 6d 65 | 899c8e8c2d9b99b
| 0140 6c 65 61 76 65 6c 6f 6e 65 72 69 6e 67 74 6f | eed56c67....Z.Q=
| 0150 6f 66 20 74 69 6d 65 6d 69 6e 67 74 6f 6c 65 | ......e.b.c.<
| 0160 66 69 6c 65 6d 65 63 61 6c 73 74 69 6e 67 74 6f | /8c2d9b99beed56
| 0170 65 6e 63 65 73 74 61 74 69 6e 67 74 6f 6c 65 | c67....zd.Y.
| 0180 6f 66 20 74 69 6d 65 6d 69 6e 67 74 6f 6c 65 | ...},#{.H..J...
| 0190 66 69 6c 65 6d 65 63 61 6c 73 74 69 6e 67 74 6f | }.5u.t......#+2.
| 01a0 65 6e 63 65 73 74 61 74 69 6e 67 74 6f 6c 65 | 8e8c2d9b99beed5
| 01b0 63 6f 6e 64 69 66 69 6e 67 74 6f 6c 65 6d 65 | 6c67........f9.
| 01c0 6f 66 20 74 69 6d 65 6d 69 6e 67 74 6f 6c 65 | L..../.hc.
| 01d0 66 69 6c 65 6d 65 63 61 6c 73 74 69 6e 67 74 6f | ...;oS56c67....me
| 01e0 66 69 6c 65 6d 65 63 61 6c 73 74 69 6e 67 74 6f | cloudshark#
| 01f0 66 69 6c 65 6d 65 63 61 6c 73 74 69 6e 67 74 6f | ....Ex........

```
chord=PUT&login=admin&password=cloudshark#.*$
```
50% done
But it’s heap memory

In the OpenSSL heap:
- Copies of the private key (full & partial)
- Moduli of the private key
Guaranteed exploitable

From: Ted Unangst <tedu <at> tedunangst.com>
Subject: Re: FYA: http://heartbleed.com/
Newsgroups: gmane.os.openbsd.misc
Date: 2014-04-08 19:27:48 GMT (2 weeks, 9 hours and 3 minutes ago)

On Tue, Apr 08, 2014 at 15:09, Mike Small wrote:
> nobody <openbsd.as.a.desktop <at> gmail.com> writes:
> 
> >> "read overrun, so ASLR won't save you"
> 
> > What if malloc's "G" option were turned on? You know, assuming the
> > subset of the worlds' programs you use is good enough to run with that.

No. OpenSSL has exploit mitigation countermeasures to make sure it's
exploitable.
What’s at risk of exposure

- usernames and passwords
- cookie values
- user provided data = \{credit card numbers, private information, email addresses\}
- encryption keys \(\text{(repeatedly confirmed)}\)

… anything that can be sent to a web server

… anything in process memory that includes LibSSL/OpenSSL
Not just your web server

- Load balancers
- VPN gateways
- Routers
- Switches
- VoIP devices
- Multiple web software packages
- Mail gateways
- Managed FTP
- TOR!!!
- Anything that uses OpenSSL/LibSSL <1.01f
TTT → Time To Tools

- Perl, python, ruby scripts ~ 24 hours
- Metasploit - same day
- Testing websites ~ 24 hours
- Automatic cert stealer (heartleech) ~ 7 days
This sounds horrible

CVSSv2 = 5??
CVSS V2 scoring evaluates the impact of the vulnerability on the host where the vulnerability is located. When evaluating the impact of this vulnerability to your organization, take into account the nature of the data that is being protected and act according to your organization’s risk acceptance. While CVE-2014-0160 does not allow unrestricted access to memory on the targeted host, a successful exploit does leak information from memory locations which have the potential to contain particularly sensitive information, e.g., cryptographic keys and passwords. Theft of this information could enable other attacks on the information system, the impact of which would depend on the sensitivity of the data and functions of that system.
Your IPS sigs

- Initial logic designed to catch specific tests
- Detection during handshake versus post-handshake
- Flag is outside encrypted payload
Heartbeat Flag

TLS version

Length = 80

Encrypted Payload

RAW Packet (encrypted payload)

Decrypted payload

Ben Sapiro (CC-BY-SA), 2014
Your logs probably won’t help

● activity won’t show in HTTP logs
● this isn’t an error alert condition (the process doesn’t abend)
● OpenSSL needs to be compiled to enable debug logging
● Mod_SSL default log level is none

Packet captures do help (if you have keying material)
Fix all the things

1. Patch OpenSSL
2. Patch LibSSL
3. Update firmware or software packages
4. Replace Keys
5. Reset in scope passwords

While you’re at it:
6. Enable Perfect Forward Secrecy
7. Disable weak ciphers
But wait, there’s more!

- Reverse Heartbleed
- Client side Heartbleed

Heartbleed is not server specific, the RFC for SSL Heartbeats is bi-directional only specifying peers in the session
Lessons Learned - AppSec/DevSec

1. Don’t rely on user provided length values
2. Length check buffers before copying
3. Static Analysis didn’t catch this
4. Set ASSERTS or equivalent
5. C is powerful, C requires careful handling
6. Code reviews are your friend
7. Don’t invent your own memory management
8. Don’t spray keying material all over process memory
Lessons Learned - Security & Ops

1. Have a complete system inventory
2. Have a complete software inventory
3. Be able to patch in 24 hours
4. Have (practiced) Incident Response processes
5. Load balancers/reverse proxies might be a good thing
6. You may like your CERT vendor less now
In summary

- Heartbleed is a vuln with a logo
- It is that bad
- Patch everywhere, replace certs, follow incident response process, reset affected passwords & sessions, start drinking
- Don’t forget your internal systems
Other takeaways

- Ignore vendors who tell you their product would have detected Heartbleed & Stuxnet
- OpenSSL needs a cleanup, audit & funding
- 19 year old script kiddies need to learn how to use TOR
- 19 year script kiddies shouldn’t annoy the government agency with all the money
Homework

- Why is Akamai’s patch broken?
- What are Theo De Raadt and the OpenBSD crew up to?
- Checkout the Cloudflare Challenge
Mandatory plug

- Go to www.kpmg.ca/cybersecurity
- Look on the right
- Download “What is Heartbleed?”
- Give to executive/management types
More Plugs

LIQUIDMATRIX

OpenCERT Canada

semper vigilantem

BOSSIDES

Ben Sapiro (CC-BY-SA), 2014
This Slide Unintentionally Blank
Thank you

This work is licensed under the Creative Commons Attribution-ShareAlike 3.0 Unported License. To view a copy of this license, visit http://creativecommons.org/licenses/by-sa/3.0/ or send a letter to Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.
Sorry