

# Heartbleed

## The Live Action Monologue

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



Rights of pictures per copyright holder/creator

# *OpenSSL* *1.0.1*



# Ben Sapiro =



# 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

# **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);
```



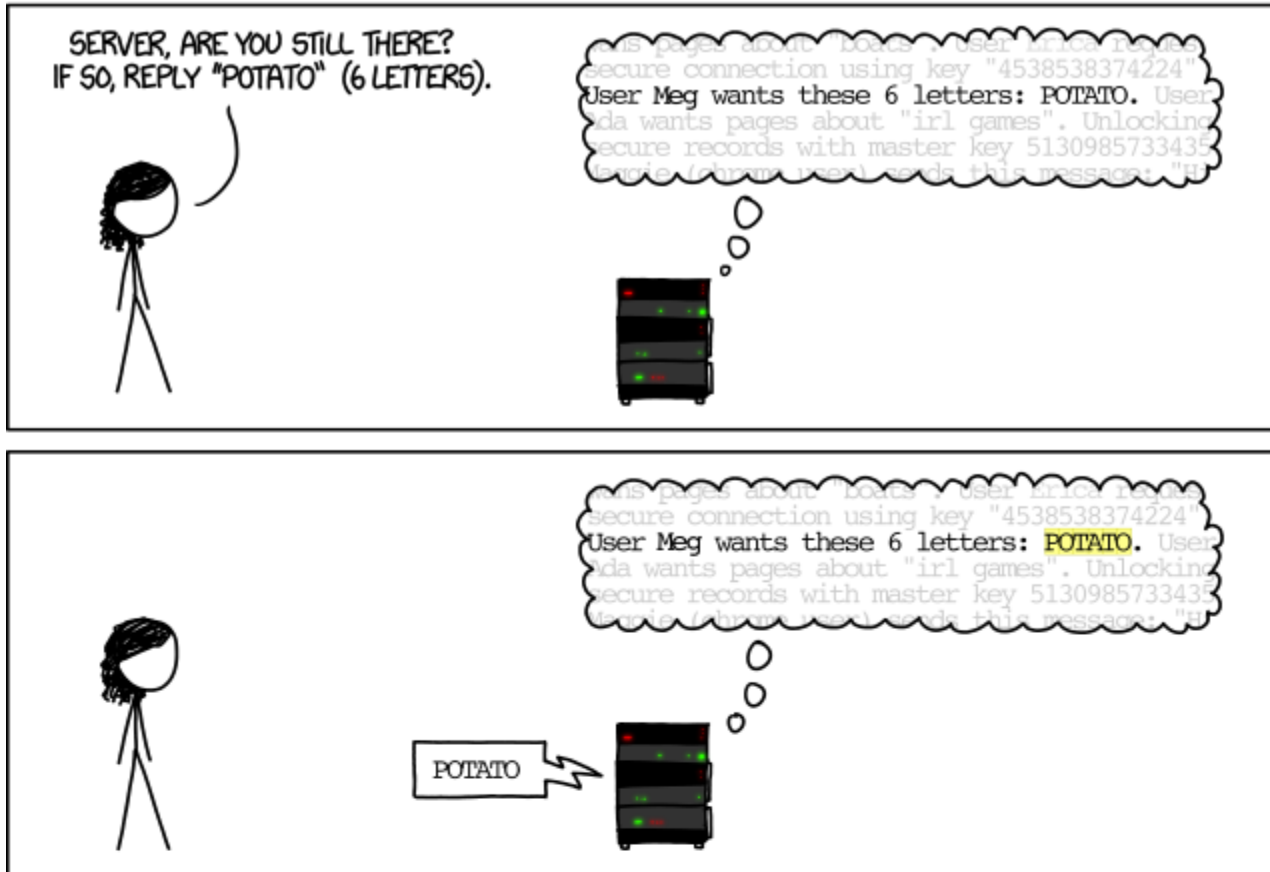
User controlled

# What is not

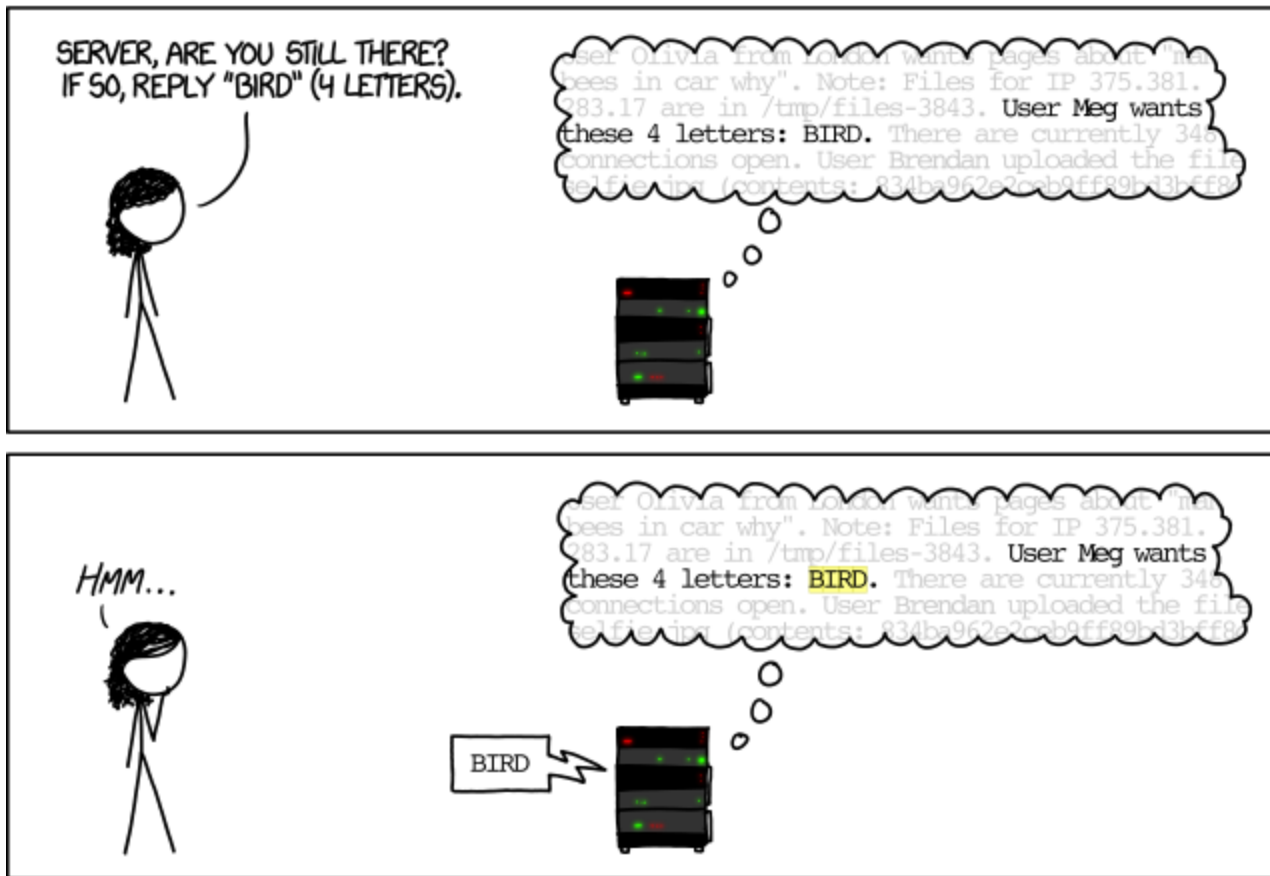
- It is not a virus
- It is not a flaw in SSL or TLS
- It is not a flaw in any cipher suite
- It does not affect all web sites
- Does not directly impact other software outside of OpenSSL/LibSSL
- It is not an issue with all versions of OpenSSL
- It is not a BoF, ROP or any other voodoo

# XKCD explains

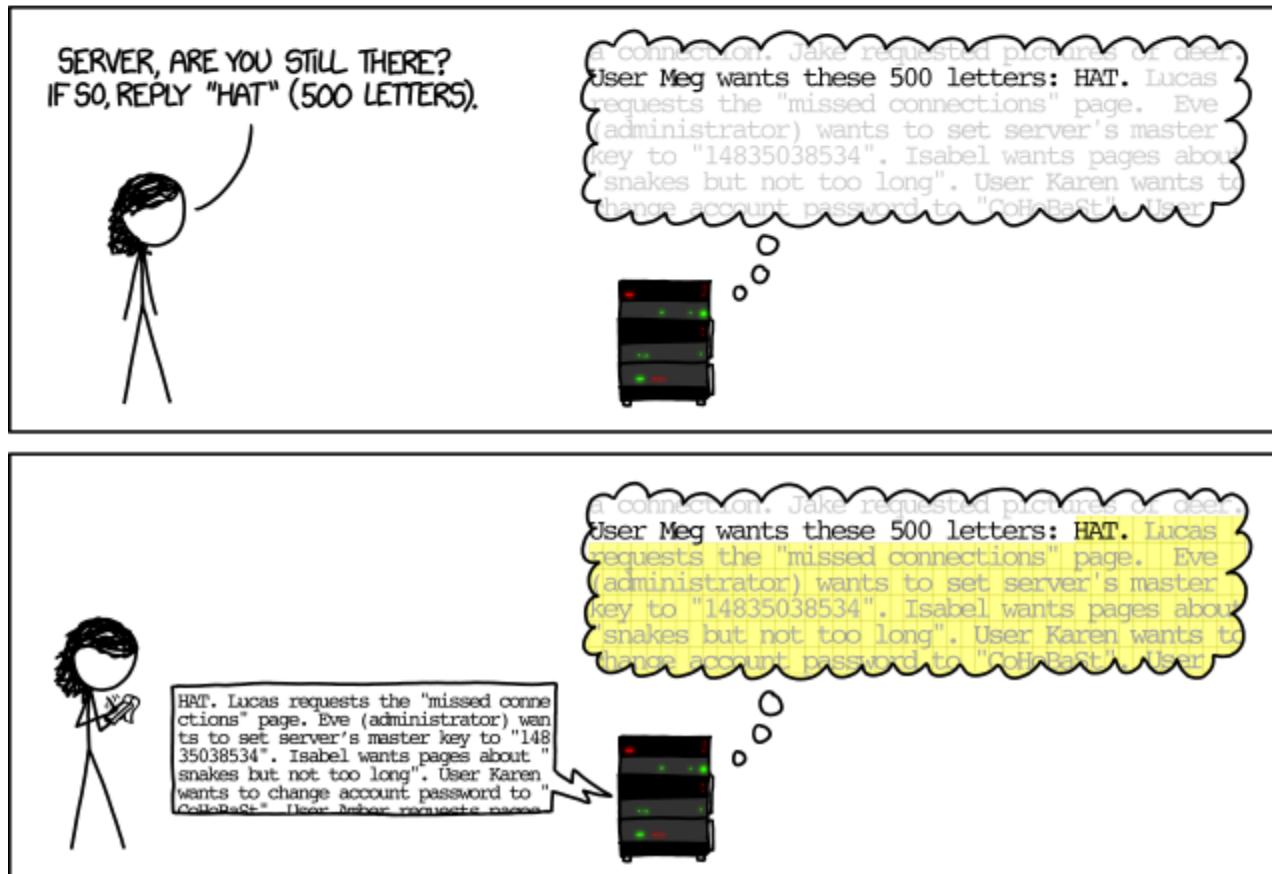
## HOW THE HEARTBLEED BUG WORKS:



# XKCD explains



# XKCD explains

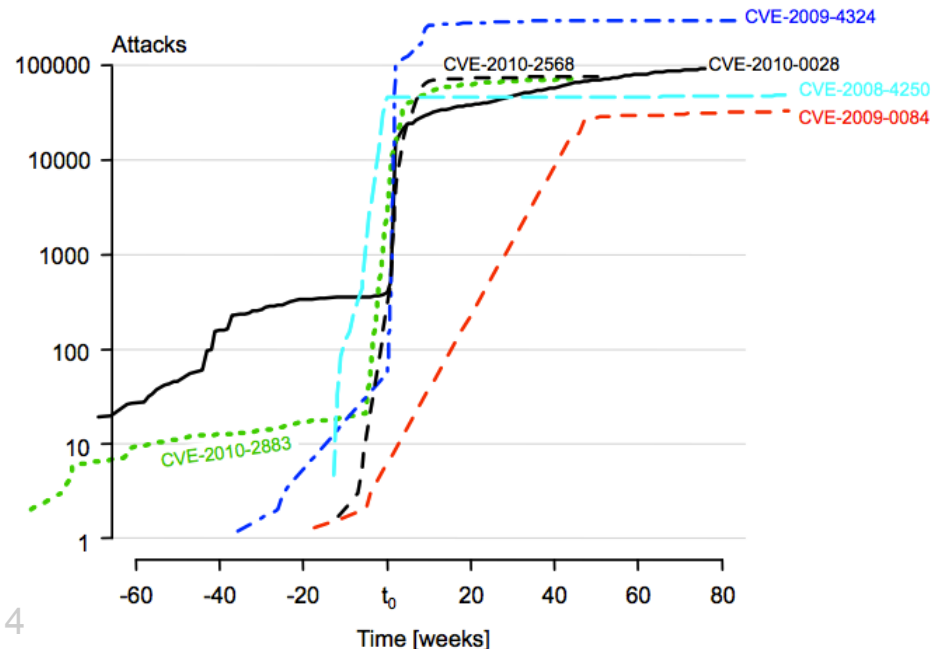


# At least two discoverers of 2 year old vulnerability

@neelmehta of



๕ CODENOMICON



# 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



Frame (1159 bytes)	Decrypted SSL record (1040 bytes)
0000	02 03 fd 68 65 61 72 74 62 6c 65 65 64 2e 66 69 ...heartbleed.fi
0010	6c 69 70 70 6f 2e 69 6f 59 45 4c 4c 4f 57 20 53 lippo.ioYELLOW S
0020	55 42 4d 41 52 49 4e 45 27 19 8d bd c6 d3 3d b3 UBMARINE'.....=.
0030	f6 44 b1 1f fb 61 14 73 0e f4 d1 96 03 03 03 03 .D...a.s.....
0040	f4 5d 50 82 82 b5 eb 68 28 53 60 69 fc b6 94 21 .]P....h(S`i...!
0050	a1 7e 7a 68 16 be 9c d6 0f ec d0 b1 00 4c 82 4a .~zh.....L.J
0060	bc e5 f0 1b 3c df bc d9 df 05 22 e8 75 d7 9e f5 ....<....."u...
0070	d8 40 83 47 55 0e 18 10 07 07 07 07 07 07 07 .@.GU.....
0080	2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f -Agent: Mozilla/
0090	35 2e 30 20 28 4d 61 63 69 6e 74 6f 73 68 3b 20 5.0 (Macintosh;
00a0	49 6e 74 65 6c 20 4d 61 63 20 4f 53 20 58 20 31 Intel Mac OS X 1
00b0	30 5f 39 5f 32 29 20 41 70 70 6c 65 57 65 62 4b 0_9_2) AppleWebKit
00c0	69 74 2f 35 33 37 2e 33 36 20 28 4b 48 54 4d 4c it/537.36 (KHTML
00d0	2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29 20 43 68 , like Gecko) Ch
00e0	72 6f 6d 65 2f 33 33 2e 30 2e 31 37 35 30 2e 31 rome/33.0.1750.1
00f0	35 32 20 53 61 66 61 72 69 2f 35 33 37 2e 33 36 52 Safari/537.36
0100	0d 0a 52 65 66 65 72 65 72 3a 20 68 74 74 70 73 ..Referer: https
0110	3a 2f 2f 63 73 2d 73 63 72 65 65 6e 73 68 6f 74 ://cs-screenshot
0120	2e 6c 61 6e 2f 63 61 70 74 75 72 65 73 0d 0a 41 .lan/captures..A
0130	63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 ccept-Encoding:
0140	67 7a 69 70 2c 64 65 66 6c 61 74 65 2c 73 64 63 gzip,deflate,sdc
0150	68 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 h..Accept-Langua
0160	67 65 3a 20 65 6e 2d 55 53 2c 65 6e 3b 71 3d 30 ge: en-US,en;q=0
0170	2e 38 0d 0a 43 6f 6f 6b 69 65 3a 20 5f 73 65 73 .8..Cookie: _ses
0180	73 69 6f 6e 5f 69 64 3d 64 66 35 63 35 64 38 37 sion_id=df5c5d87
0190	38 39 39 63 38 65 38 63 32 64 39 62 62 39 39 62 899c8e8c2d9bb99b
01a0	65 65 64 35 36 63 36 37 0d 0a 0d 0a 5a 95 51 3d eed56c67....Z.Q=
01b0	ae 96 f9 b4 14 c3 65 f6 a0 94 62 b1 63 a1 03 3c .....e...b.c...<
01c0	2f 38 63 32 64 39 62 62 39 39 62 65 65 64 35 36 /8c2d9bb99beed56
01d0	63 36 37 0d 0a 0d 0a 7a 3f 64 d9 bf c0 13 59 7f c67....z?d....Y.
01e0	92 98 b8 7e 91 2c 7d 8c 23 a7 48 1e d6 4a a2 ee ...~.,}.#.H..J..
01f0	7d 1a 95 35 75 f3 16 74 9a a3 1d b7 23 2b 32 11 }..5u..t....#+2.
0200	38 65 38 63 32 64 39 62 62 39 39 62 65 65 64 35 8e8c2d9bb99beed5
0210	36 63 36 37 0d 0a 0d 0a d1 bf ca be 66 39 d5 8b 6c67.....f9..
0220	4c c4 dd 29 ac c1 ea 1d 1c 20 19 2f b1 68 63 fb L..). .... ./..hc.
0230	18 3b 6f 53 35 36 63 36 37 0d 0a 0d 0a 5f 6d 65 .;oS56c67.... me
0240	74 68 6f 64 3d 50 55 54 26 6c 6f 67 69 6e 3d 61 thod=PUT&login=a
0250	64 6d 69 6e 26 70 61 73 73 77 6f 72 64 3d 63 6c dmin&password=cl
0260	6f 75 64 73 68 61 72 6b 23 13 2a 85 7f 17 ad a3 oudshark#.*.....
0270	5c 15 b0 8e d0 94 45 78 00 00 00 00 00 00 00 \.....Ex.....

**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: **[gmmane.os.openbsd.misc](http://gmmane.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 (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



Sponsored by  
DHS National Cyber Security Division/US-CERT



NIST  
National Institute of  
Standards and Technology

## National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Vulnerabilities	Checklists	800-53/800-53A	Product Dictionary	Impact Metrics	Data Feeds	Statistics
Home	SCAP	SCAP Validated Tools	SCAP Events	About	Contact	Vendor Comments

### Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

### Resource Status

NVD contains:

- 61744 [CVE Vulnerabilities](#)
- 231 [Checklists](#)
- 248 [US-CERT Alerts](#)
- 2854 [US-CERT Vuln Notes](#)
- 10286 [OVAL Queries](#)
- 87696 [CPE Names](#)

Last updated: 4/20/2014  
CVE Publication rate: 19.5

### Email List

NVD provides four mailing lists to the public. For information and subscription instructions please visit [NVD Mailing Lists](#)

### Workload Index

## National Cyber Awareness System

### Vulnerability Summary for CVE-2014-0160

**Original release date:** 04/07/2014  
**Last revised:** 04/19/2014  
**Source:** US-CERT/NIST

### Overview

The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1\_both.c and t1\_lib.c, aka the Heartbleed bug.

### Impact

**CVSS Scoring (version 2.0):**

**CVSS v2 Base Score:** 5.0 (MEDIUM) (AV:N/AU:N/C:P/AV:A/AC:L/Au:N/C:P/Impact:High)

**Impact Subscore:** 2.9

**Exploitability Subscore:** 10.0

### CVSS Version 2 Metrics:

**Access Vector:** Network exploitable

**Access Complexity:** Low

**Authentication:** Not required to exploit


**Impact Type:** Allows unauthorized disclosure of information

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.


CVSSv2 = 5??



# This sounds horrible



Sponsored by  
DHS National Cyber Security Division/US-CERT



NIST  
National Institute of  
Standards and Technology

## National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Vulnerabilities	Checklists	800-53/800-53A	Product Dictionary	Impact Metrics	Data Feeds	Statistics
Home	SCAP	SCAP Validated Tools	SCAP Events	About	Contact	Vendor Comments

### Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

### Resource Status

**NVD contains:**  
61744 [CVE Vulnerabilities](#)  
231 [Checklists](#)  
248 [US-CERT Alerts](#)  
2854 [US-CERT Vuln Notes](#)  
10286 [OVAL Queries](#)  
87696 [CPE Names](#)

Last updated: 4/20/2014  
CVE Publication rate: 19.5

### Email List

NVD provides four mailing lists to the public. For information and subscription instructions please visit [NVD Mailing Lists](#)

### Workload Index

## National Cyber Awareness System

### Vulnerability Summary for CVE-2014-0160

**Original release date:** 04/07/2014  
**Last revised:** 04/19/2014

**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.****

**Impact Type:** Allows unauthorized disclosure of information

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

0000	00	90	0b	12	91	c1	a8	86	dd	a3	f9	75	08	00	4		
0010	00	89	6c	82	40	00	40	06	15	11	ac	10	01	8a	0		
0020	01	42	ec	73	01	bb	40	b7	e1	ea	30	6a	c4	9c	80	18	.B.s..@...0j....
0030	20	00	c5	1b	00	00	01	01	08	0a	0f	90	66	7d	00	53	.....f}.S
0040	d9	b8	18	03	03	00	50	c0	c8	a3	79	44	fc	39	92	e2	.....P...yD.9..
0050	07	98	e3	fa	76	92	c7	c6	04	b9	13	6e	16	62	b5	b4	....v.....n.b..
0060	81	ee	60	48	b7	b7	99	a4	69	1a	71	09	c5	3f	f2	28	..`H....i.q..?.(
0070	b0	1c	e5	35	9a	e3	96	d7	70	72	7f	96	71	f4	29	d6	...5....pr..q.).
0080	9d	a4	70	e3	d0	01	ff	fd	a4	bd	9b	ef	d2	d9	9c	72	..p.....r
0090	bc	5f	86	8a	fa	17	54										._....T

RAW Packet (encrypted payload)

Heartbeat  
Flag

TLS  
version

Length = 80

Encrypted Payload



Frame (151 bytes)																Decrypted SSL record (40 bytes)																
0000	01	03	fd	68	65	61	72	74	62	6c	65	65	64	2e	66	69	...heartbleed.fi															
0010	6c	69	70	7	6f	2e	69	6f	59	45	4c	4c	4f	57	20	53	lippo.ioYELLOW S															
0020	55	42	4d	41	52	49	4e	45									UBMARINE															

Decrypted payload

Type

Length = 1021

# 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](http://www.kpmg.ca/cybersecurity)
- Look on the right
- Download “What is Heartbleed?”
- Give to executive/management types

The screenshot shows the KPMG Canada website. The header includes the KPMG logo, the tagline "cutting through complexity", and navigation links for "Canada - English", "News", "Contact Us", and a search bar. A secondary navigation bar lists "About", "Topics", "Industries", "Services", "Research", "Careers", "Partners", and "Alumni".

The main content area is titled "Cyber Security" and features a large image of a circuit board. Below the image, text states: "The threats from cyber adversaries are continuing to grow in scale and sophistication. Public and private organizations in various sectors worldwide now openly acknowledge that cyber attacks are one of the most prevalent and high impact risks they face." Further down, it mentions "Canada's Cyber Security Strategy is a cornerstone of our Government's commitment to keep Canada – including our cyberspace – safe, secure and prosperous." and "Dealing with cyber threats is a complex challenge. Much of the current focus is on protection and compliance, as organizations – subject to increasing amounts of legislative, corporate and regulatory requirements – demonstrate they are managing and protecting information appropriately." The bottom of the main content area begins with "However, the Information Security landscape is constantly evolving. Despite the recognition of the risks posed by cyber threats, private and public sector organizations find it difficult to believe they could be a target for cyber attacks. Many of the risks and impacts of cyber attacks are shared between the Government and private sector. For example, untrustworthy technology is harmful to".

On the right sidebar, under the "Contact us" section, there is a profile for Kevvie M. Fowler, Partner, Advisory Services, Forensic, with contact information: 416-777-3742 and a link to "Contact by e-mail". Below this, a red box highlights a section titled "What is Heartbleed?" which includes a download link for a PDF document titled "Heartbleed - Identifying and managing the risk".

# More Plugs



**LIQUIDMATRIX**



**OpenCERT Canada**

semper vigilan<sup>tem</sup>



**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

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.

