

Forum:[Hack Forums](#)

Thread: [\[READ\] \[2/3 of PASSWORDS EXPOSED\] All internet passwords exposed.](#)

thehen101 - April 9, 2014, 7:43 am

Change your passwords for everything.

So as some of you may know, a few hours ago a bug in SSL was made public. This bug is called heartbleed, and affected 2/3 of the internet by exploiting memory leaks to give the hacker usernames, passwords and content. As I am a nice person, I just wanted to warn users about this, and I strongly urge everyone reading this to change thier password for everything, as I am doing now.

There probably are other threads about this, but all users may not still be aware.

Read up on this more:

<http://www.theepochtimes.com/n3/609175-heart-bleed-bug-imperils-web-encryption-putting-passwords-credit-cards-at-risk/>

<http://heartbleed.com/>

<http://www.theguardian.com/technology/2014/apr/08/heartbleed-bug-puts-encryption-at-risk-for-hundreds-of-thousands-of-servers>

<http://www.bbc.co.uk/news/technology-26935905>

<http://lifel hacker.com/what-the-heartbleed-security-bug-means-for-you-1560801201>

xhflhkeuhwguu34 - April 9, 2014, 7:45 am

Uh.

There has been no proof of a hacker exploiting this in the wild.

If you have 2FA you shouldn't be bothered by this either.

Rem - April 9, 2014, 7:45 am

I read about this just a little while ago, and I was surprised. However, I was too lazy to change passwords, lol.

thehen101 - April 9, 2014, 7:47 am

(Apr 9, 2014 07:45 AM)Xen0n Wrote: [\[CITE\]](#) Uh.

There has been no proof of a hacker exploiting this in the wild.

If you have 2FA you shouldn't be bothered by this either.

No, but read the second link and you will see that people could hack themselves.

~Jay~ - April 9, 2014, 7:47 am

It isn't necessarily true that two thirds of all passwords have been leaked, just that two thirds of servers used the vulnerable software. There's no guarantee that the servers were vulnerable, or even the vulnerable ones you used were hacked, or that your password was in the memory dump when it was hacked. They don't even know if heartbleed was widely used or not.

thehen101 - April 9, 2014, 7:51 am

(Apr 9, 2014 07:47 AM)??????????? Wrote: [\[CITE\]](#) It isn't necessarily true that two thirds of all passwords have been leaked, just that two thirds of servers used the vulnerable software. There's no guarantee that the servers were vulnerable, or even the vulnerable ones you used were hacked, or that your password was in the memory dump when it was hacked. They don't even know if heartbleed was widely used or not.

This bug had been known for 2 years, and a few hours ago many, many people were made aware of it. Of course there is no guarantee (as the bug leaves no trace), but there is a huge chance.

xhflhkeuhwguu34 - April 9, 2014, 7:54 am

(Apr 9, 2014 07:51 AM)thehen101 Wrote: [\[CITE\]](#) This bug had been known for 2 years, and a few hours ago many, many people were made aware of it. Of course there is no guarantee (as the bug leaves no trace), but there is a huge chance.

It has not been known for two years.

It may have been in the code for two years but certainly not known.

Tony S - April 9, 2014, 8:00 am

No.

First of all, I think 2/3 of websites/services on the Internet being vulnerable is an extremely far-fetched and stupid guesstimation especially given that there is no evidence to back this claim up. A large portion of the top 1000 Alexa-ranked sites didn't even use SSL whatsoever, and most of the ones that did fixed the bug within no time.

Even IF two thirds of every service that used OpenSSL is (or was) vulnerable at one point, it doesn't mean that all of their base were stolen. Large corporations such as Cloudflare and Google along with software distributors were pre-notified of the vulnerability so that they could prepare fixed and patches for release on disclosure day, meaning a lot of services that were vulnerable fixed it straight away, and the large majority of other websites/services that were vulnerable managed to fix it in no time whatsoever since they have dedicated teams that look at stuff like this.

With that being said, there were still a vast amount of websites/services that had been exploited maliciously and this happening had been brought to the attention of the public in a swift manner, two of the more notable ones being [PlentyOfFish](#) and [Yahoo!](#).

Furthermore, using the bug you're only able to grab 64kb chunks of memory from the target at one time. You're not going to get Yahoos entire userbases' data with a bug like this. There is the off chance that if it were something like a forum, a privileged user could have had their credentials/sessions stolen and attackers could have used that to leverage their own privileges.

However, I think that if a large company which millions of people use knows that they are affected by this, they will be smart enough to take the proper precautions needed to ensure that the integrity of their users isn't going to be violated. Whether this be resetting password for everyone that logged in during a specific time, resetting users sessions or just notifying them that their data might have been compromised.

Null Byte - April 9, 2014, 9:24 am

I change all my passwords every month or two, so I guess I'll do it early this April. Good heads up, OP.

Ap?? - April 9, 2014, 9:32 am

Heartbleed only allow's the attacker to grab 64K of memory. Sure it can be ran over and over again but it would take a GREAT amount of time to do this to multiple websites on the web. I posted an

example of the heartbleed exploit dump.

Spoiler ([Click to View](#))

```
Code root@aprose:/var# python tst.py 127.0.0.1
```

```
Connecting...
```

```
Sending Client Hello...
```

```
Waiting for Server Hello...
```

```
... received message: type = 22, ver = 0302, length = 58
```

```
... received message: type = 22, ver = 0302, length = 1010
```

```
... received message: type = 22, ver = 0302, length = 525
```

```
... received message: type = 22, ver = 0302, length = 4
```

```
Sending heartbeat request...
```

```
... received message: type = 24, ver = 0302, length = 16384
```

```
Received heartbeat response:
```

```
0000: 02 40 00 D8 03 02 53 43 5B 90 9D 9B 72 0B BC 0C .@....SC[...r...
```

```
0010: BC 2B 92 A8 48 97 CF BD 39 04 CC 16 0A 85 03 90 .+..H...9.....
```

```
0020: 9F 77 04 33 D4 DE 00 00 66 C0 14 C0 0A C0 22 C0 .w.3....f.....".
```

```
0030: 21 00 39 00 38 00 88 00 87 C0 0F C0 05 00 35 00 !.9.8.....5.
```

```
0040: 84 C0 12 C0 08 C0 1C C0 1B 00 16 00 13 C0 0D C0 ..... 
```

```
0050: 03 00 0A C0 13 C0 09 C0 1F C0 1E 00 33 00 32 00 .....3.2.
```

```
0060: 9A 00 99 00 45 00 44 C0 0E C0 04 00 2F 00 96 00 ....E.D...../...
```

```
0070: 41 C0 11 C0 07 C0 0C C0 02 00 05 00 04 00 15 00 A.....
```

```
0080: 12 00 09 00 14 00 11 00 08 00 06 00 03 00 FF 01 ..... 
```

```
0090: 00 00 49 00 0B 00 04 03 00 01 02 00 0A 00 34 00 ..l.....4.
```

```
00a0: 32 00 0E 00 0D 00 19 00 0B 00 0C 00 18 00 09 00 2.....
```

```
00b0: 0A 00 16 00 17 00 08 00 06 00 07 00 14 00 15 00 ..... 
```

```
00c0: 04 00 05 00 12 00 13 00 01 00 02 00 03 00 0F 00 ..... 
```

```
00d0: 10 00 11 00 23 00 00 00 0F 00 01 01 60 79 47 62 ....#.....`yGb
```

```
00e0: 1C 58 A0 A8 C2 CF 70 37 C0 B8 80 6D 2B 9A D6 B7 .X....p7...m+...
```

```
00f0: 97 3F CD 46 2D F6 18 39 34 AC 20 2A 66 8E 66 0C .?.F--..94. *f.f.
```

```
0100: FB 7F 89 58 02 DC 51 D5 C8 E3 58 7F 15 9C 0A 50 ...X..Q...X....P
```

```
0110: DF 4A F4 9B A2 E3 FA B2 2B 38 94 22 83 8D 62 46 .J.....+8.."..bF
```

```
0120: C8 55 35 50 18 4B 36 BB 57 6F DF 98 E2 20 BF 19 .U5P.K6.Wo... ..View Full Dump @
```

<http://pastebin.com/rDNKkduH>

thehen101 - April 9, 2014, 9:47 am

(Apr 9, 2014 09:32 AM)Ap?? Wrote: ([CITE](#)) Heartbleed only allow's the attacker to grab 64K of memory. Sure it can be ran over and over again but it would take a GREAT amount of time to do this to multiple websites on the web. I posted an example of the heartbleed exploit dump.

Spoiler ([Click to View](#))

```
Code root@aprose:/var# python tst.py 127.0.0.1
```

```
Connecting...
```

```
Sending Client Hello...
```

```
Waiting for Server Hello...
```

```
... received message: type = 22, ver = 0302, length = 58
```

```
... received message: type = 22, ver = 0302, length = 1010
```

```
... received message: type = 22, ver = 0302, length = 525
```

```
... received message: type = 22, ver = 0302, length = 4
```

```
Sending heartbeat request...
```

```
... received message: type = 24, ver = 0302, length = 16384
```

```
Received heartbeat response:
```

0000: 02 40 00 D8 03 02 53 43 5B 90 9D 9B 72 0B BC 0C .@....SC[...r...
0010: BC 2B 92 A8 48 97 CF BD 39 04 CC 16 0A 85 03 90 .+..H...9.....
0020: 9F 77 04 33 D4 DE 00 00 66 C0 14 C0 0A C0 22 C0 .w.3....f.....".
0030: 21 00 39 00 38 00 88 00 87 C0 0F C0 05 00 35 00 !.9.8.....5.
0040: 84 C0 12 C0 08 C0 1C C0 1B 00 16 00 13 C0 0D C0
0050: 03 00 0A C0 13 C0 09 C0 1F C0 1E 00 33 00 32 00 3.2.
0060: 9A 00 99 00 45 00 44 C0 0E C0 04 00 2F 00 96 00 E.D...../...
0070: 41 C0 11 C0 07 C0 0C C0 02 00 05 00 04 00 15 00 A.....
0080: 12 00 09 00 14 00 11 00 08 00 06 00 03 00 FF 01
0090: 00 00 49 00 0B 00 04 03 00 01 02 00 0A 00 34 00 ..l.....4.
00a0: 32 00 0E 00 0D 00 19 00 0B 00 0C 00 18 00 09 00 2.....
00b0: 0A 00 16 00 17 00 08 00 06 00 07 00 14 00 15 00
00c0: 04 00 05 00 12 00 13 00 01 00 02 00 03 00 0F 00
00d0: 10 00 11 00 23 00 00 00 0F 00 01 01 60 79 47 62#.....`yGb
00e0: 1C 58 A0 A8 C2 CF 70 37 C0 B8 80 6D 2B 9A D6 B7 .X....p7...m+...
00f0: 97 3F CD 46 2D F6 18 39 34 AC 20 2A 66 8E 66 0C .?.F--..94. *f.f.
0100: FB 7F 89 58 02 DC 51 D5 C8 E3 58 7F 15 9C 0A 50 ...X..Q...X....P
0110: DF 4A F4 9B A2 E3 FA B2 2B 38 94 22 83 8D 62 46 .J.....+8."..bF
0120: C8 55 35 50 18 4B 36 BB 57 6F DF 98 E2 20 BF 19 .U5P.K6.Wo... ..View Full Dump @
<http://pastebin.com/rDNKkduH>

Yeah, that shows that it is possible. This has been in circulation for a while, and even though the chance that many people affected is small, there's still a chance. If a group of people were to concentrate on one server for a while, sooner or later they would strike gold and reveal sensitive information.

Aura - April 9, 2014, 9:50 am

OKAY STOP POSTING NEW THREADS ABOUT THIS EVERY HOUR.

We already have 3-4 threads dedicated to this, USE THEM.

xhflhkeuhwguu34 - April 9, 2014, 9:52 am

(Apr 9, 2014 09:50 AM)Aur? Wrote: [\[CITE\]](#) OKAY STOP POSTING NEW THREADS ABOUT THIS EVERY HOUR.

We already have 3-4 threads dedicated to this, USE THEM.

you should make a thread telling people to stop making threads about it

thehen101 - April 9, 2014, 9:56 am

(Apr 9, 2014 09:52 AM)Xen0n Wrote: [\[CITE\]](#) you should make a thread telling people to stop making threads about it

I originally posted this in the lounge, I'm actually quite glad there are threads about this because it shows that people on HF still have a small amount of 'care for the community'.

Some websites are still vulnerable:

<http://filippo.io/Heartbleed/#avazutracking.net>

Aura - April 9, 2014, 9:56 am

(Apr 9, 2014 09:52 AM)Xen0n Wrote: [\[CITE\]](#) you should make a thread telling people to stop making threads about it

I'm about to do it. Just take all the fucking threads and put them in one.

jde1126 - June 16, 2014, 1:53 pm

lol. I was hoping this was easily replicated.

Caillou - June 16, 2014, 1:55 pm

(Jun 16, 2014 01:53 PM)jde1126 Wrote: [\[CITE\]](#) lol. I was hoping this was easily replicated.
Thank you for posting on something from 2 months ago.

Aura - June 16, 2014, 2:05 pm

(Jun 16, 2014 01:55 PM)Caillou Wrote: [\[CITE\]](#) Thank you for posting on something from 2 months ago.

About a flaw that has been fixed around 2 months ago.
Damn new users.