

## Forum:[Hack Forums](#)

Thread: [\[ALERT\] CloudFlare vulnerability | #Cloudbleed HTTPS Traffic Leak](#)

**Pulz** - February 23, 2017, 8:36 pm

Source from discord: Liberal clam(Programmix#0748)

Just a heads up of a recently exposed vulnerability within CloudFlare's infrastructure. The vulnerability pertains to data exposure during transmission between CloudFlare's proxy servers and the target server. This has been the case for data transferred between 2016-09-22 and 2017-02-18.

Discord's Aethex developer, 'Liberal clam' made the announcement on his server within the hour of this post.

Passwords should be changed on all sites using CloudFlare.

Discord itself is listed as an affected site, but Discord confirmed that they are unlikely to have been affected as they do not use the features of CloudFlare that were vulnerable. But your password should be changed anyway, just for safety.

Affected sites and more information can be found in this list:

<https://github.com/pirate/sites-using-cloudflare>

Liberal's sources:

<https://bugs.chromium.org/p/project-zero/issues/detail?id=1139>

<https://blog.cloudflare.com/incident-report-on-memory-leak-caused-by-cloudflare-parser-bug/>

[https://www.reddit.com/r/sysadmin/comments/5vu3yn/cloudbleed\\_seceurity\\_bug\\_cloudflare\\_reverse/](https://www.reddit.com/r/sysadmin/comments/5vu3yn/cloudbleed_seceurity_bug_cloudflare_reverse/)

Edit | Some interesting news articles have popped up:

[https://www.theregister.co.uk/2017/02/24/cloudbleed\\_buffer\\_overflow\\_bug\\_spaffs\\_personal\\_data/](https://www.theregister.co.uk/2017/02/24/cloudbleed_buffer_overflow_bug_spaffs_personal_data/)

<https://medium.com/@octal/cloudbleed-how-to-deal-with-it-150e907fd165#.ahn7wcd5a>

<https://www.lifehacker.com.au/2017/02/cloudflare-cloudbleed-bug-exposes-sensitive-data-who-is-affected/>

<https://www.privateinternetaccess.com/blog/2017/02/cloudflares-cloudbleed-worst-privacy-leak-recent-internet-history/>

Omniscient Wrote:Got this from CF today...

Quote:Quote:

Your domain is not one of the domains where we have discovered exposed data in any third party caches. The bug has been patched so it is no longer leaking data.

**Ainaj** - February 23, 2017, 8:39 pm

Got it in 20 seconds before me..

**Eternal.** - February 23, 2017, 8:45 pm

This is a serious breach, I recommend changing your passwords pretty much everywhere because

even if the site itself wasn't affected, it could have used a site connected to cloudflare and been leaked.

**Ainaj** - February 23, 2017, 8:46 pm

I some reason sensed something like this yesterday and changed most important passwords

**W?lr??** - February 23, 2017, 8:48 pm

Wait about a weeks worth of time and this will be all over the news just like heartbleed

**Ainaj** - February 23, 2017, 9:02 pm

Oh and CC info could be exposed too. RIP.

**vaiperboy** - February 23, 2017, 9:04 pm

hackforums is on that list :|

my 2fa will still protect me, right? (unless if the secret key is stolen as well)

even <https://www.authy.com/> is on that list Imfao, fuckin rip us

**Ace of Knaves** - February 23, 2017, 9:05 pm

So many BTC sites on that list that could be affected (Coinbase, Localbitcoins, Poloniex). Potential for a lot of money to go 'missing'...

**SIM-888979** - February 23, 2017, 9:06 pm

(Feb 23, 2017 10:04 PM)vaiperboy Wrote: [\[CITE\]](#) hackforums is on that list :|

my 2fa will still protect me, right?

We'll have to wait for Omniscient to confirm this.

**Pulz** - February 23, 2017, 9:07 pm

(Feb 23, 2017 09:48 PM)W?lr?? Wrote: [\[CITE\]](#) Wait about a weeks worth of time and this will be all over the news just like heartbleed

Maybe. CloudFlare claims only a small percentile of requests were 'leaked', but then again, you never know if your own data was included.

**Ainaj** - February 23, 2017, 9:11 pm

(Feb 23, 2017 10:06 PM)Aurora Wrote: [\[CITE\]](#) We'll have to wait for Omniscient to confirm this.

Every website that uses Cloudflare, and any part of their service that modifies the HTML code has been affected. So yes, this includes HF

**SIM-888979** - February 23, 2017, 9:14 pm

(Feb 23, 2017 10:11 PM)CesarVB Wrote: [\[CITE\]](#) Every website that uses Cloudflare, and any part of their service that modifies the HTML code has been affected. So yes, this includes HF

I thought it was only websites that uses specific features of CloudFlare such as email obfuscation, server-side Excludes and automatic HTTPS rewrites.

<https://blog.cloudflare.com/incident-report-on-memory-leak-caused-by-cloudflare-parser-bug/>

Perhaps HF does not have those features enabled?

**J?son** - February 23, 2017, 9:16 pm

general idea how bad this is

**Ainaj** - February 23, 2017, 9:19 pm

(Feb 23, 2017 10:14 PM)Aurora Wrote: [\[CITE\]](#) I thought it was only websites that uses specific features of CloudFlare such as email obfuscation, server-side Excludes and automatic HTTPS rewrites.

<https://blog.cloudflare.com/incident-report-on-memory-leak-caused-by-cloudflare-parser-bug/>

Perhaps HF does not have those features enabled?

Pretty sure Omni mentioned he was trying the HTTPS rewrites for something, around the time he moved to https

**Pulz** - February 23, 2017, 9:26 pm

I don't pretend to understand exactly what features and requirements have to be met in order to be part of the whole Cloudbleed problem, so it's pretty possible that many sites on the list- including HF, weren't affected at all. But still, passwords should be changed regularly anyway. So nows a better time than any.

**Ainaj** - February 23, 2017, 9:32 pm

(Feb 23, 2017 10:26 PM)Pulz Wrote: [\[CITE\]](#) I don't pretend to understand exactly what features and requirements have to be met in order to be part of the whole Cloudbleed problem, so it's pretty possible that many sites on the list- including HF, weren't affected at all. But still, passwords should be changed regularly anyway. So nows a better time than any.

Passwords are not the only thing leaked here.

Everything sent via your http request had the chance to be leaked, including backing information, private bitcoin keys, pictures/nudes, pretty much anything you do online has the chance to be included in this leak.

Your real ip is included with this leak too, so once all the information is collected it could be possible to see your browsing habits.

Also your gauth private keys could be exposed, API keys, private messages on dating sites. Heck even password managers are affected, exposing ALL your passwords/address/cc info etc

It's bad.

**Pulz** - February 23, 2017, 9:35 pm

(Feb 23, 2017 10:32 PM)CesarVB Wrote: [\[CITE\]](#) ... snip ...Yeah, the extent of it appears to be pretty severe.

I've updated the post with some new news articles that are quite interesting.

**Leroy Jethro Gibbs** - February 23, 2017, 9:53 pm

Hackforums was also on the list of vuln websites. To prevent any possible hacks via session cookies, logout then log back in. That will generate a new cookie for you.

**Ainaj** - February 23, 2017, 9:55 pm

(Feb 23, 2017 10:53 PM)Leroy Jethro Gibbs Wrote: [\[CITE\]](#)

Hackforums was also on the list of vuln websites. To prevent any possible hacks via session cookies, logout then log back in. That will generate a new cookie for you.

They're also tied to IP, so that wouldn't matter.

**Leroy Jethro Gibbs** - February 23, 2017, 10:01 pm

(Feb 23, 2017 10:55 PM)CesarVB Wrote: [\[CITE\]](#) They're also tied to IP, so that wouldn't matter. Yes it would. Omni has confirmed this in the past when I was helping him. To reset the credentials you will need to logout then back in.

**Riggs** - February 23, 2017, 10:10 pm

"This has been the case for data transferred between 2016-09-22 and 2017-02-18."

Before everyone freaks out and loses their shit, please consider the size of the site list and how much data we're talking about here. Even over an extended period of time, that's still big data even a nation state's resources would struggle to effectively comb.

**Universal.** - February 23, 2017, 10:19 pm

I still don't really get it, how can someone see other users information? I highly doubt one can just pull up the cached version of these sites and pull a random users data.

Am I missing something here?

**thrudda** - February 23, 2017, 10:22 pm

Woah, coinbase and Poloniex? Thanks for the heads up OP

**Ravioli** - February 23, 2017, 10:22 pm

Thanks for notifying all of us OP, appreciate it.

**EasyPeasy** - February 23, 2017, 10:39 pm

All my websites are affected... how do I fix this?

**thrudda** - February 23, 2017, 10:41 pm

(Feb 23, 2017 11:39 PM)EasyPeasy Wrote: [\[CITE\]](#) All my websites are affected... how do I fix this? Change all your password and activate 2FA if there is

**UglyMeister** - February 23, 2017, 10:45 pm

RIP all my favorite sites :(

**EasyPeasy** - February 23, 2017, 10:46 pm

(Feb 23, 2017 11:41 PM)thrudda Wrote: [\[CITE\]](#) Change all your password and activate 2FA if there is Anyway I can find the cache of my website or it's deleted? I want to see what has been leaked... I dont have much on my website but goddamn this is annoying, I used the feature that was leaked... arghh

**Pulz** - February 23, 2017, 10:57 pm

(Feb 23, 2017 11:46 PM)EasyPeasy Wrote: [\[CITE\]](#) Anyway I can find the cache of my website or it's deleted? I want to see what has been leaked... I dont have much on my website but goddamn this is annoying, I used the feature that was leaked... arghh

As it's already been said, the amount of data that was leaked was huge, but only accounted for a fraction of the total request by CloudFlare. The likelihood you will come across your own data is astronomical- unless someone devises a way to gather all the leaked data and then sift through it.

The point of this alert is so that you change your passwords, or reset your login tokens/session cookies on the off-chance you were affected and could be compromised.

**VirtualMon3y** - February 23, 2017, 11:22 pm

Thanks for the heads up OP. A day of resetting passwords ahead....

**Omniscient** - February 23, 2017, 11:33 pm

I wouldn't worry about this. I doubt this is going to be a big deal for most of us.

Quote:The greatest period of impact was from February 13 and February 18 with around 1 in every 3,300,000 HTTP requests through Cloudflare potentially resulting in memory leakage (that's about 0.00003% of requests).

I'd be shocked if any actual HF data was leaked. We server about a million pages a day. It lasted for 5 days. So say that's 5 million pages. That gives us about 1.5 pages we served MIGHT have had the memory leak. But then those leaked pages also have to be cached somewhere and viewable.

You may as well go play the lottery tomorrow.

And yes, I changed my CF password and API keys. That takes me 10 seconds. I don't see the need to do anything more until CF tells me to do so.

I ain't worried, so neither should you be.

btw...another instance where the false security of HTTPS fails.

**Pulz** - February 24, 2017, 12:17 am

Plus the probability of HF being served to the cache engine is very, very low. But good to hear that the impact is a lot less than the media has blown it up to be.

**Neeeeeeeeeeel.-** - February 24, 2017, 1:16 am

Omni, I also agree with you that the probability of any HF leak is too low. But the vulnerability exists since 2016-09-22 on the "Automatic HTTP Rewrites" feature, and HF has it enabled since the HTTPS was forced, that's more than 5 days.

Cloudflare blog Wrote:2016-09-22 Automatic HTTP Rewrites enabled

2017-01-30 Server-Side Excludes migrated to new parser

2017-02-13 Email Obfuscation partially migrated to new parser

2017-02-18 Google reports problem to Cloudflare and leak is stopped

**BITCHLESS** - February 24, 2017, 1:22 am

Cloudflare pointed out their bug bounty program, but I noticed it has a top-tier reward of a t-shirt.

**MightyOne** - February 24, 2017, 1:28 am

Im always scared when these sort of things happend, you can never know if your data is the date that got leaked ...

**hustle.** - February 24, 2017, 5:50 am

Damn this is wild , just changed like 10 passes lmaoo

**Darrell** - February 24, 2017, 5:51 am

Holy fuck, this will be one of the largest breaches in 2017 I bet.

**snoopydoggg** - February 24, 2017, 5:52 am

Good thing I don't use any websites that use cloudflare, not even this one.

:^)

Also nice spelling.

**Traum** - February 24, 2017, 6:05 am

Thank you for the info, changing my passwords right now. I hope HF didn't encounter any major breach that would lead to user-data to be leaked.

**Regulus** - February 24, 2017, 9:10 am

Regarding this Omnis thread here: <https://hackforums.net/showthread.php?tid=5559708>

I believe Hackforums would be safe or did I miss-read something?

**Armada** - February 24, 2017, 9:29 am

(Feb 24, 2017 10:10 AM)Regulus Wrote: [\[CITE\]](#) Regarding this Omnis thread here: <https://hackforums.net/showthread.php?tid=5559708>

I believe Hackforums would be safe or did I miss-read something?

I would imagine with 2FA your accounts fine, but its still a good idea to reset PWs.

Now I gotta remember a whole new set of codes. INB4 I get locked out of god knows how many sites.....

**Egregious** - February 24, 2017, 10:28 am

CloudFlare sent that email not only as a transparency report, but also as a form of damage control. The 150 customers they mentioned are actually not the only people who are affected. That's just a conservative estimate of the sites they were able to find, and there are many more unreported ones. Anyone using CloudFlare's server-side excludes, email obfuscation, or HTTPS re-writes may have suffered from this bug. You're wondering, "what if I don't have any of these features enabled?" The problem is that other sites who do have one or more of those features enabled were able to leak information across sites as well. An unrelated site could've had leaked sensitive information from your own domain, and some of this info could still be in various third-party caches around the world. Even Tavis, the member of Google's Project Zero team that discovered the bug, says that CloudFlare seriously downplayed the severity of the problem. At least now it has been patched.

**drip** - February 24, 2017, 10:37 am

I hope one day there will be a fb leak.

That would be crazy lol ?

**He B TeMy** - February 24, 2017, 1:07 pm

(Feb 24, 2017 11:37 AM)danjelsann Wrote: [\[CITE\]](#) I hope one day there will be a fb leak.

That would be crazy lol ?

Too bad FB is using akamai.

**LastSession** - February 24, 2017, 1:25 pm

Should I really worry about my CC?

**Armada** - February 24, 2017, 1:48 pm

(Feb 24, 2017 02:25 PM)LastSession Wrote: [\[CITE\]](#) Should I really worry about my CC?

PART of my DNS runs through CF FFS, this has me worried personally. ?

**Ainaj** - February 24, 2017, 1:51 pm

(Feb 24, 2017 02:48 PM)Armada Wrote: [\[CITE\]](#) PART of my DNS runs through CF FFS, this has me worried personally. ?

1 in 3.3m chance you were affected, don't worry my child

**Armada** - February 24, 2017, 1:53 pm

(Feb 24, 2017 02:51 PM)CesarVB Wrote: [\[CITE\]](#) 1 in 3.3m chance you were affected, don't worry my child

Your input means so much to me....

Glad to see your back to zero rep again. ?

-I repeat my same statement again, improve attitude, your gonna get further.

But thats again, just my opinion.

**Salt peter** - February 24, 2017, 1:58 pm

Looks like I'm going to have to keep a close eye on my bank accounts the next few weeks.

**Darkwin** - February 24, 2017, 2:41 pm

Well hopefully Authy isn't affected otherwise RIP to a lot of HF accounts.

**rogelio11** - February 24, 2017, 11:28 pm

that sucks. i guess we will see random people doing btc giveaways on reddit and other sites real soon lol

**A +** - February 25, 2017, 5:22 am

(Feb 23, 2017 11:19 PM)Universal. Wrote: [\[CITE\]](#) I still don't really get it, how can someone see other users information? I highly doubt one can just pull up the cached version of these sites and pull a random users data.

Am I missing something here?

I was wondering the same thing lol

**SavageAF** - February 25, 2017, 5:23 am

(Feb 23, 2017 10:06 PM)Aurora Wrote: [\[CITE\]](#) We'll have to wait for Omniscient to confirm this. Omni confirmed we were not impacted by this iirc