The CloudFlare Hack

DON'T USE CLOUDFLARE

Cloudflare Data Leak: How to Secure Your Site

This entry was posted in General Security, WordPress Security on February 23, 2017 by Mark Maunder 23 Replies

Cloudflare has experienced a data leak over a 5 month period that mixed sensitive data between websites and visitors. A visitor to one website using Cloudflare may have seen data from another website using Cloudflare that was being sent to a completely different site visitor.

Some of the leaked data has been indexed by search engines who have been working over the past few days to try and remove the data from their caches.

In this post I am going to explain in simple terms, what occurred and what you need to do about it.

If you are a WordPress user and simply want to know how to secure your site, you can skip to the What Should I Do section below. I have included some information for non-WordPress site owners in that section too.

What Happened in the Cloudflare Data Leak?

Cloudflare provides a firewall and content distribution service. Their servers are between your website visitors and your own web server.

Under normal circumstances, cloudflare returns the data each site visitor requested to that visitor. This may be public or sometimes private information and it is usually done over a secure channel. Each website visitor only sees the data they requested.

From September 22nd, 2016 until February 18th 2017 (last Saturday), Cloudflares servers in some cases mixed data that belonged to one visitor to a website, with data belonging to another visitor that was visiting a completely different website.

The worst data leakage occurred between the dates of February 13th and February 18th when one in every 3.3 million requests to Cloudflare's servers was leaked.

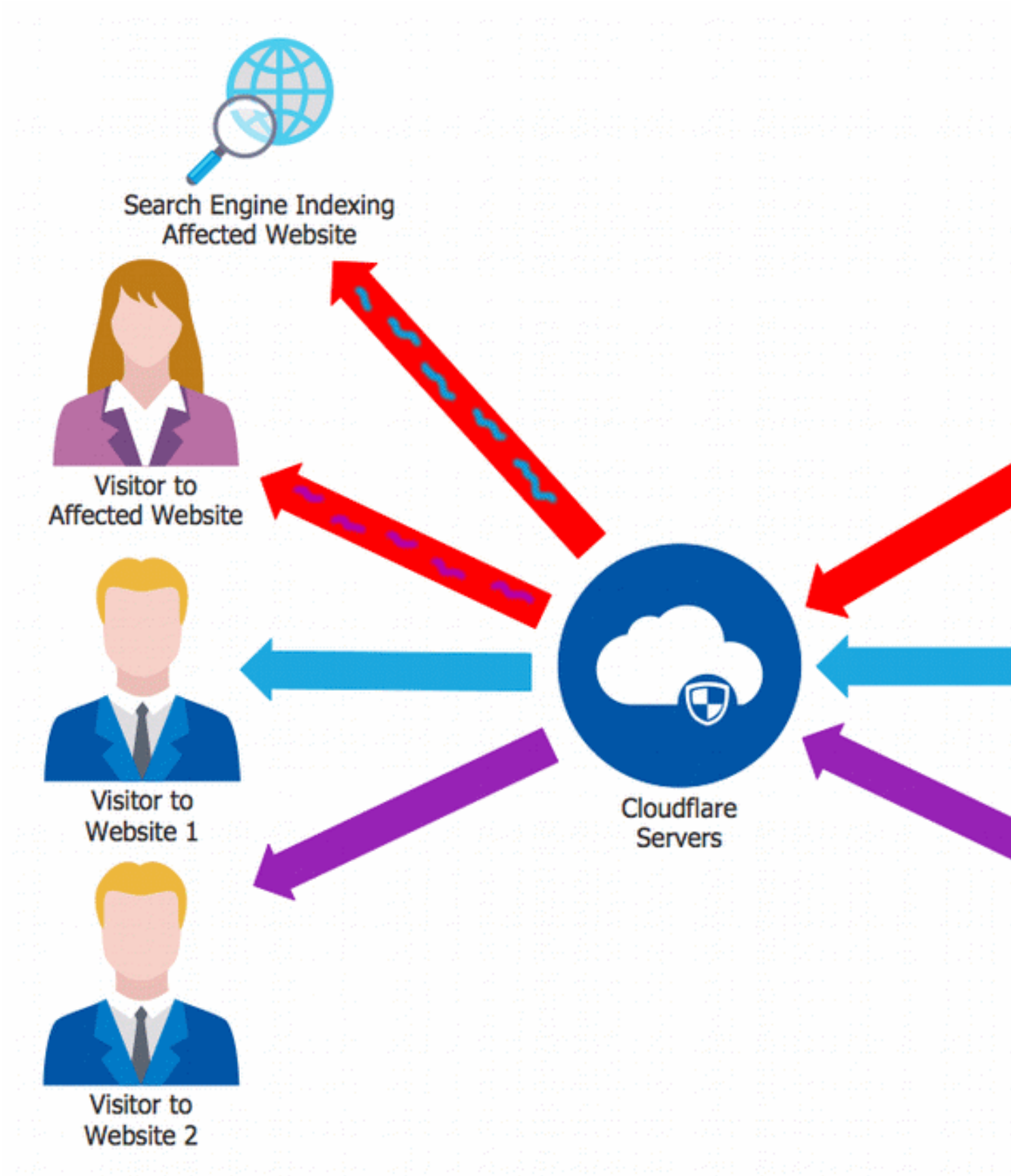
During the period when the leak occurred, visitors to certain websites would see what appeared to be garbage data mixed into the web page they were viewing. That garbage data was data from a memory leak. The data was in some cases sensitive and included security tokens and other sensitive information.

According to Tavis Ormandy, the researcher who discovered this data leak:

“The examples we’re finding are so bad, I cancelled some weekend plans to go into the office on Sunday to help build some tools to cleanup. I’ve informed cloudflare what I’m working on. I’m finding private messages from major dating sites, full messages from a well-known chat service, online password manager data, frames from adult video sites, hotel bookings. We’re talking full https requests, client IP addresses, full responses, cookies, passwords, keys, data, everything.”

Data leakage occurred when a site visitor or search engine visited one of 3438 domains hosted behind Cloudflare’s servers, according to Cloudflare’s CTO who posted a comment on Hacker News. However, **any of Cloudflare’s customer websites could have had their response data mixed into data returning from those 3438 websites**. Tavis Ormandy confirms this in the same Hacker News thread.

You can see an illustration of this data leakage in the diagram below. Any visitor to an ‘affected website’ which is one of the 3438 websites, could have had data from any one of over 5 million Cloudflare customer sites mixed into their response. Website 1 and Website 2 which are not ‘affected’ websites could have experienced data leakage to visitors of the ‘affected’ website.


Search Engine Indexing
Affected Website
Visitor to
Affected Website
Visitor to
Website 1
Visitor to
Website 2
Cloudflare
Servers

What Data Was Leaked?

The data that was leaked could include passwords, cookies and authentication tokens. If an attacker is able to access the text of your cookies, they may be able to use them to sign into your website.

Internal Cloudflare private keys used to secure data being transferred between Cloudflare machines were also leaked.

At this point one should assume that there is a small chance that any private data transferred from any Cloudflare customer website to a site visitor may have been leaked between September 2016 and February of this year.

According to Cloudflare, no private SSL customer keys were leaked from the memory of their servers. A private SSL key is a key used to secure visitor connections to your website. If the your private SSL key is leaked, an attacker could listen in on all traffic to and from your website.

Has the Leaked Data Been Stored Somewhere?

Unfortunately Google and other search engines have been crawling the web during the time that this leak was occurring on Cloudflare's systems. Those search engines stored the leaked data when they indexed one of the 3438 affected websites.

When viewing cached pages in Google, it is still possible at the time of writing (7pm Pacific Time on Feb 23rd) to view cached sensitive data in Google's search results.

Similarly it is possible to view sensitive Cloudflare data in DuckDuckGo’s search results.

Since this leak was discovered, Google and other search engines have been working to try and remove the sensitive data from their caches. Based on what we are seeing this evening, there is still some data that needs to be removed.

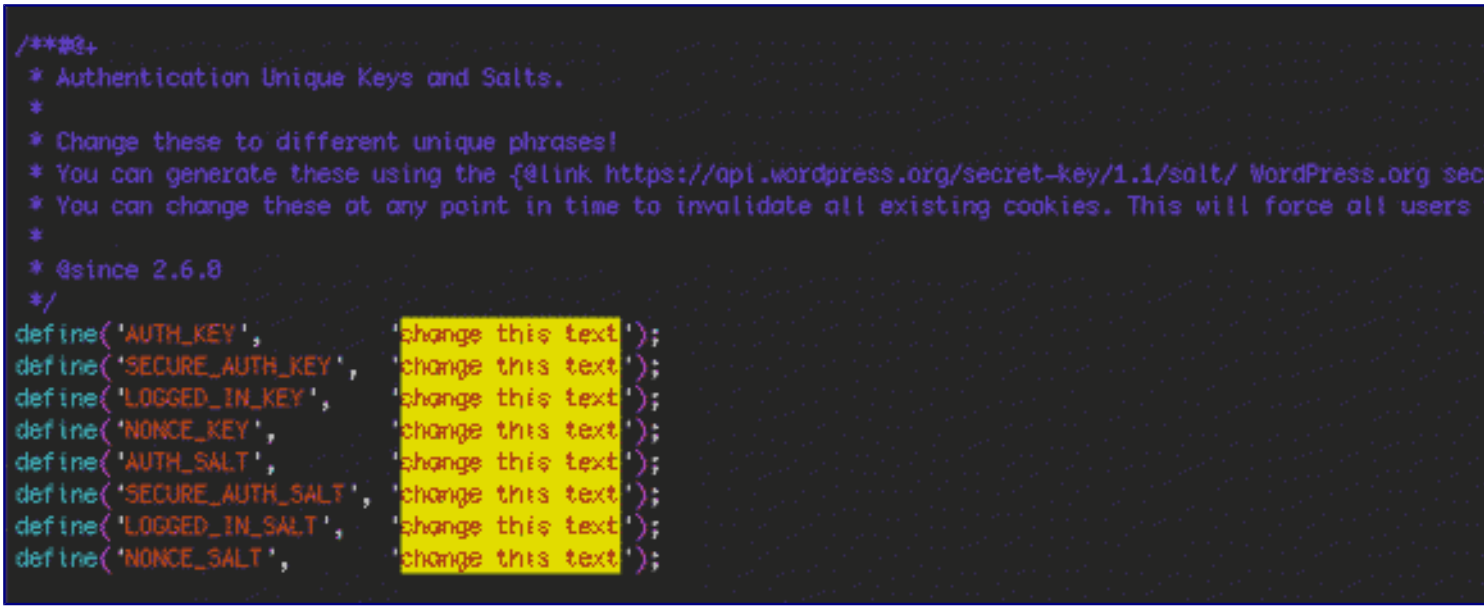
What Should I Do if I use Cloudflare on my Website?

According to a conversation on Hacker News between the Cloudflare CTO and Tavis Ormandy, the security researcher who discovered this, any customer of Cloudflare's could have been affected by this data leak.

WordPress site owners: Change your wp-config.php salts. This will log everyone out and invalidate cookies and sessions

If you are using WordPress, we recommend you edit your wp-config.php file and change all of the 'salts'. This will automatically log all of your users out. This protects you and your site members in case any of their cookies have been stolen. Once you make this change, an attacker will no longer be able to use stolen session cookies from your site to sign in.

You need to change the following section in your wp-config.php and save it:



We suggest that you change the highlighted text in your wp-config.php to a long random string of characters and numbers. You can also use the link in the comment above the ‘define’ statements to generate a salt.

Non-WordPress Site Owners: Invalidate Sessions

If you use a different publishing platform, you will need to ensure that all sessions are invalidated. That means that your site visitor login cookies need to be made invalid. You will need to consult the documentation of your particular publishing platform to determine how to do this.

Suggest your site members change their passwords and change your Admin passwords

As a precautionary measure, you should suggest that your site members change their passwords. You should also change any admin level passwords.

You may need to comply with any data breach reporting requirements you have

This bug in Cloudflare’s systems is being described as a “data leak”. It is unclear at this point whether it is considered a “data breach”. A private database of customer personally identifiable information was not stolen. However, private data that may have included customer PII was leaked, no matter how small.

If you have HIPAA, PCI or other reporting requirements that relate to data breaches, you may want to get advice on whether you are required to report this incident.

Check the Search Results

It is difficult to determine if any private information from your site has been stored in the search results. However, we recommend that as a precautionary measure you do a few Google searches with your domain name in quotes. Add the following text to the search:

```
-site:example.com
```

Replace example.com with your own site domain. Take note of the minus sign before the word ‘site’ above. This will exclude results from your own website. You can exclude results from other sites using the same operator several times. You can also try adding the following in quotes:

“CF-Host-Origin-IP:”

If you do find any results, report them immediately to Google for removal.

Who Discovered This and How?

Tavis Ormandy discovered this data leak in Cloudflare’s systems. He is a security researcher employed by Google’s Project Zero. Project Zero is a Google team who works on trying to find zero day (previously unknown) vulnerabilities.

Tavis discovered the data leak while analyzing Google search results. He noticed data that appeared to be a raw memory dump and he and his colleagues took a closer look and discovered it was a data leak in Cloudflare’s servers that was leaking data between websites.

Tavis is a well known researcher who has done ground breaking research in the computer security field over the past few years.

Has This Problem Been Fixed by Cloudflare?

The Cloudflare team have fixed the data leak on February 18th which was last Saturday. You can find a detailed technical post on Cloudflare’s blog describing what caused the leak and how it was fixed.

According to Techcrunch, Cloudflare have not notified customers like Uber and OkCupid directly.

Where Else Can I Read About This?

The following are the most authoritative resources discussing this issue:

- The thread on the Project Zero mailing list where Tavis discloses the issue.
- The Cloudflare blog. This is a highly technical post describing how they fixed the issue.
- The Hacker News thread that first brought public attention to this issue.

Google Accidentally Resets Routers To Default Configuration (Google has backdoors into WiFi and OnHub devices) (thurrott.com)

submitted ago by seeprime to technology (+41|-0)