PDF Export for report 1436047

Sourcemap Exposure on Less Visited Pages

State	Informative
Reported by	Emir (dirt3009)
Reported to	Spotify (spotify)
Submitted at	(ISO-8601)
Asset	*.spotify.com (URL)
References	
Weakness	Remote File Inclusion
Severity	none
CVE IDs	

Most subdomains/pages that are visited less than the most have their sourcemap files exposed.

3 examples I have found to this are:
payments.spotify.com
surveys.spotify.com
works.spotify.com

While I cannot know what caused sourcemaps to slip-through on these deployments I'm pretty sure this may happen again if not regulated on newer deployments.

Impact

Full or partial access to the source-code of the frontend deployment.

Activity

Hi @dirt3009,

Thanks for your report. Based on your initial description, there do not appear to be any security implications as a direct result of this behavior.

The described behavior poses no risk.

If you disagree, please reply with additional information describing your reasoning. Including a working proof-of-concept is the best way to convey the impact of this report and will streamline our assessment of your claims.

Kind regards,
@offs1de

Offside	2021-12-26 11:36	bug not applicable	Public

Exposure of sourcemaps on public deployments can have multiple implications, as far as infosec goes sourcemaps may reveal removed pieces of code, credentials and links to pages that should not be viewable by the public. On the business side this may create an unfair advantage giving rivals the ability to audit and clone Spotify's intellectual code.

As you have stated there are no security impliciations I shall be publishing the reconstructed sources of these pages publicly, I will be waiting for your reconsideration.

Emir	2021-12-26 12:40	comment	Public

Hi @dirt3009,

Please provide proof-of-concept for the behavior your are describing with screenshot/URLs..etc

Thanks,
@offs1de

Offside	2021-12-26 12:55	comment	Public

Due to the nature of this this cannot be described py a screenshot but here's a simple explanation.

First off let's start by what a a sourcemap is, as MDN states this is what a sourcemap is:
A source map is a file that maps from the transformed source to the original source, enabling the browser to reconstruct the original source and present the reconstructed original in the debugger.

So let's start off by the 3 examples I have provided, first comes**surveys.spotify.com**

We'll need a tool like Postman for this instance since the server does not send us the sourcemap if we try accessing it with a standard browser the service worker that's running on the page will mock a 404 page. After we have the sourcemap file we can use many of the utilities that can be used to reconstruct these sourcemaps, my favorite projects for these are unwebpack-sourcemap and Webpack Exploder.

Feeding the file sourcemap file into one of these tools will spit out the source code, that the webpack was compiled from, to their respected files with the same relative file hierarchy that was used on the source.

Next, as an example for a webapp built with Next.js we'll take a look at**payments.spotify.com**

First off we will call
```
webpackChunk_N_E
```
on our browser console to obtain all the javascript files that were used in the webpack, then we will append
```
.map
```
at the ends of these files and again use any utility to obtain the source.

Same goes for the final example at **works.spotify.com**

We find the js files that were used by inspecting the page as a webpack was not callable from the browser's dev console then we repeat the same steps.

If you have any questions do not hesitate to ask further.

Emir	2021-12-26 13:26	comment	Public

Offside	2021-12-26 14:19	bug reopened	Public

Hi @dirt3009,

I'm totally appreciate the provided information, however; you haven't show a reproduction steps to demonstrates the behavior. Please include the affected URLs, the command to use with postman and the tools you have mentioned, this help use determine the duplicate reports too.. You report missing important information and we will not be able to validate your report.

Best,
@offs1de

Offside	2021-12-26 14:21	bug needs more info	Public

As a simple proof of concept, let's use surveys.spotify.com sourcemaps.

First of all we will open Postman and send a GET request to
```
https://surveys.spotify.com/static/js/main.87db24e7.js.map
```
since this is the sourcemap file.
Then we will click **Save Response** on the response window of Postman, we will save the response as
```
main.87db24e7.js.map
```

We will then use Webpack Exploder located at https://spaceraccoon.github.io/webpack-exploder, we will click on the blue**Select** button and select the sourcemap file.
After the proccessing is finished a file called output.zip will be created with the recreation of the source from the sourcemap file.

If you have any further questions we can get in a Zoom/Teams meeting, I'll gladly explain.

Emir	2021-12-26 15:41	bug new	Public

Hey @dirt3009,

After review, there doesnâ€™t seem to be any security risk and/or security impact as a result of the behavior you are describing.

For this scenario to be considered as a valid security vulnerability you need to demonstrate the security impact such as access to sensitive information.

If you are able to leverage this into a practical exploitation scenario, we will be happy to reevaluate this report, but at this time, it does not present a significant security risk.

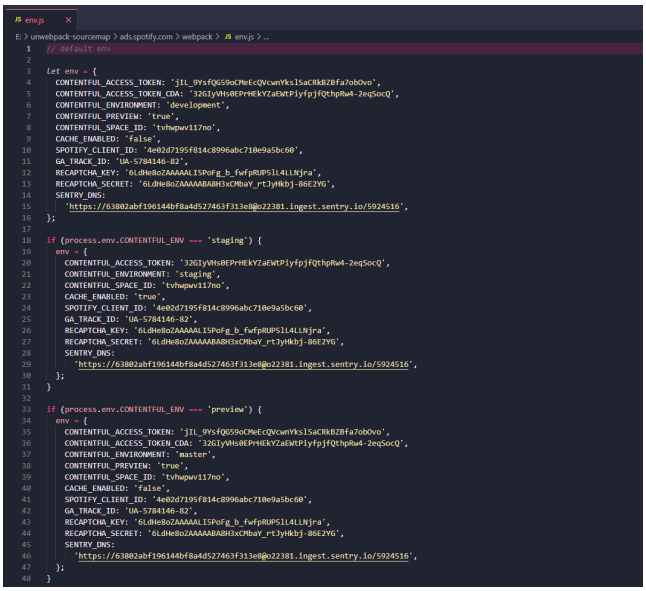
As a result, we will be closing this report as informative. This will not have any impact on your Signal or Reputation score. We appreciate your effort and look forward to seeing more reports from you in the future.

Kind regards,
@offs1de

Offside	2021-12-27 12:10	bug informative	Public

I have found a page where it actually poses a risk. This example exposes keys such as the contentful access token and the recaptcha secret. As "it does not present a significant security risk" I will be publishing it publcly in couple of hours unless this report is acknowledged.

unknown_(6).png



Emir	2021-12-27 20:38	comment	Public

Since the writing of my last message I have realized that it sounds cocky and threatening. This was not what I went for.

It's just that well knowing this can lead to a secret exposure I report it, it looks unrealistic to you, and couple hours later I actually find an exposure caused by it.

Looking forward to hearing from you and my sincere apologies.
dirt3009

Emir	2021-12-28 05:35	comment	Public

Hi, I'm still waiting.

Emir	2021-12-28 08:25	comment	Public

Hi @dirt3009,

Please feel free to dig on that and find out how an attacker could get from this token. If you are able to leak any data that arenâ€™t mean to be public using this tokens, I will be happy to take another look in your report.

Best,
@offs1de

Offside	2021-12-28 09:57	comment	Public