PDF Export for report 1437087

Sourcemaps Expose The Env.js File

State	N/A
Reported by	Emir (dirt3009)
Reported to	Spotify (spotify)
Submitted at	(ISO-8601)
Asset	*.spotify.com (URL)
References	
Weakness	Use of Hard-coded Credentials
Severity	high
CVE IDs	

First of all I want to start this report off by referring to another sourcemap report that was rejected and flagged as informative at #1436047

Now let's get to the report, ads.spotify.com has all the sourcemaps exposed they don't have any access control just sitting there to he accessed, using these sourcemaps I was able to get keys/credentials such as the contentful key and Google CAPTCHA secret.

Impact

As stated in my last report a sourcemap exposure may have many effects, sometimes this is just a competitor being able to take a look at your tech and sometimes it can cause exposures like this.

Activity

Thank you for your report, @dirt3009.

Although your finding might appear to be a security vulnerability, after reviewing your submission it appears this behavior does not pose a concrete and exploitable risk to the platform in and on itself, as Javascript libraries are meant to be public. If you're able to demonstrate any impact using the "keys" you claim to have obtained please let us know, and provide an accompanying working exploit.

Your effort is nonetheless appreciated and we wish that youâ€™ll continue to research, and submit any future security issues you find.

Cheers,
@still

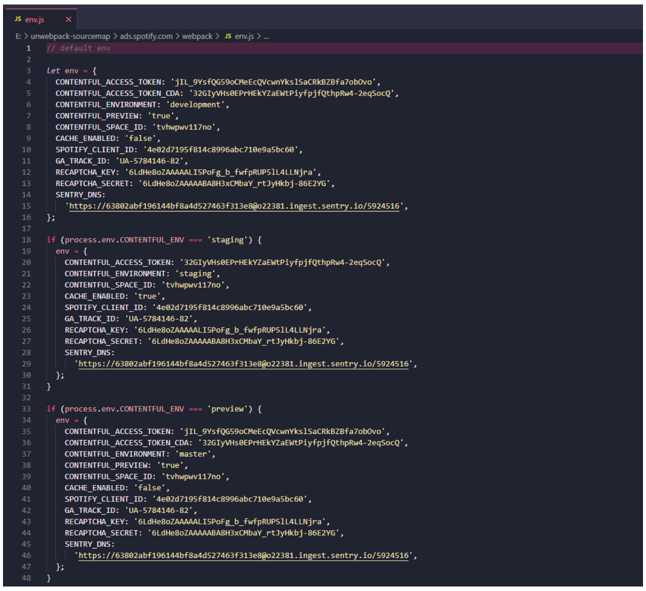
2021-12-28 09:09 bug not applicable Public

I do not think you "reviewed" anything, this is not a JavaScript library, this is a configuration file viewable publicly.

Please refer to the screenshot along with the contentful and recaptcha docs to understand why you simply don't push such keys to production, don't hardcode them get them from an environment variable that is never pushed.

I'd like to chat with an actual in-house Spotify security engineer instead of a triage because you and the last triage are simply underqualified to understand anything.

unknown_(6).png


env.js
E: > unwebpack-sourcemap > ads.spotify.com > webpack > env.js > ...

```
// default env

let env = {
  CONTENTFUL_ACCESS_TOKEN: 'jIL_9YsfQG59oCMeEcQVcwnYkslSaCRkBZBfa7obOvo',
  CONTENTFUL_ACCESS_TOKEN_CDA: '32GIyVHs0EPrHEkYZaEWtPiyfpjfQthpRw4-2eqSocQ',
  CONTENTFUL_ENVIRONMENT: 'development',
  CONTENTFUL_PREVIEW: 'true',
  CONTENTFUL_SPACE_ID: 'tvhwpwv117no',
  CACHE_ENABLED: 'false',
  SPOTIFY_CLIENT_ID: '4e02d7195f814c8996abc710e9a5bc60',
  GA_TRACK_ID: 'UA-5784146-82',
  RECAPTCHA_KEY: '6LdHe8oZAAAAALI5PoFg_b_fwfpRUP5lL4LLNjra',
  RECAPTCHA_SECRET: '6LdHe8oZAAAAABA8H3xCMbaY_rtJyHkbj-86E2YG',
  SENTRY_DNS:
    'https://63802abf196144bf8a4d527463f313e8@o22381.ingest.sentry.io/5924516',
};

if (process.env.CONTENTFUL_ENV === 'staging') {
  env = {
    CONTENTFUL_ACCESS_TOKEN: '32GIyVHs0EPrHEkYZaEWtPiyfpjfQthpRw4-2eqSocQ',
    CONTENTFUL_ENVIRONMENT: 'staging',
    CONTENTFUL_SPACE_ID: 'tvhwpwv117no',
    CACHE_ENABLED: 'true',
    SPOTIFY_CLIENT_ID: '4e02d7195f814c8996abc710e9a5bc60',
    GA_TRACK_ID: 'UA-5784146-82',
    RECAPTCHA_KEY: '6LdHe8oZAAAAALI5PoFg_b_fwfpRUP5lL4LLNjra',
    RECAPTCHA_SECRET: '6LdHe8oZAAAAABA8H3xCMbaY_rtJyHkbj-86E2YG',
    SENTRY_DNS:
      'https://63802abf196144bf8a4d527463f313e8@o22381.ingest.sentry.io/5924516',
  };
}

if (process.env.CONTENTFUL_ENV === 'preview') {
  env = {
    CONTENTFUL_ACCESS_TOKEN: 'jIL_9YsfQG59oCMeEcQVcwnYkslSaCRkBZBfa7obOvo',
    CONTENTFUL_ACCESS_TOKEN_CDA: '32GIyVHs0EPrHEkYZaEWtPiyfpjfQthpRw4-2eqSocQ',
    CONTENTFUL_ENVIRONMENT: 'master',
    CONTENTFUL_PREVIEW: 'true',
    CONTENTFUL_SPACE_ID: 'tvhwpwv117no',
    CACHE_ENABLED: 'false',
    SPOTIFY_CLIENT_ID: '4e02d7195f814c8996abc710e9a5bc60',
    GA_TRACK_ID: 'UA-5784146-82',
    RECAPTCHA_KEY: '6LdHe8oZAAAAALI5PoFg_b_fwfpRUP5lL4LLNjra',
    RECAPTCHA_SECRET: '6LdHe8oZAAAAABA8H3xCMbaY_rtJyHkbj-86E2YG',
    SENTRY_DNS:
      'https://63802abf196144bf8a4d527463f313e8@o22381.ingest.sentry.io/5924516',
  };
}
```

Emir	2021-12-28 09:20	comment	Public