Content Security Policies For ReachDeck and SpeechStream

Last Modified on Thursday, 04-May-2023 13:56:58 BST

Content Security Policies are becoming increasingly common on websites. They are intended to prevent code being injected into your website, control cross-site scripting and prevent clickjacking and other code injection attacks.

Because our products are third party scripts you install on your website, it is possible for a CSP to stop our products working correctly. You may need to adjust your CSP to allow the code to work.

ReachDeck and SpeechStream 2.5.4 supports strict CSPs that disallow the use of evals and inline scripts. However, we still need to use certain media types and files from third party locations to function on your website.

Find out more about Content Security Policies.

You may also want to add the below domains to your firewall or content filters if you are working within a locked down network.

Recommended ReachDeck CSP

This is the default CSP that we recommend you use to integrate ReachDeck. Specific parts of this will be explained below.

A CSP can be applied on a page in a meta tag or in a http response header set on the web server. It is up to the website owner to decide the best way to implement their CSP.

This CSP assumes that ReachDeck is loaded with secure protocol (https) and on a secure site and the website is using the Best Practice ReachDeck Configuration.

Updates to Policy are highlighted in red.

```
default-src
  'self';
 style-src
  'self'
  'unsafe-inline'
  https://www.browsealoud.com
  https://plus.browsealoud.com;
 Script-src
  https://plus.browsealoud.com
  https://www.browsealoud.com
  https://*.speechstream.net
  https://www.googletagmanager.com/
  https://www.google-analytics.com/
  https://apis.google.com
  https://wikisum.texthelp.com/
 'sha256-aEDmoObzmjNv962J42VzD3ELW5yetlhKLnYGA32/4aU=';
 img-src
  https://browsealoud-webservices-8.texthelp.com/
  https://browsealoud-webservices-eu.texthelp.com/
  https://www.browsealoud.com
  'self'
  https://plus.browsealoud.com
  https://upload.wikimedia.org
  https://www.google-analytics.com/
  https://stats.g.doubleclick.net
  data:;
 child-src
  'self'
  https://content.googleapis.com
  https://www.googletagmanager.com/ns.html;
 Connect-src
  blob:
  https://plus.browsealoud.com/
  https://www.browsealoud.com
  https://en.wikipedia.org/
  https://wikisum.texthelp.com/
  https://wiki-summarizer-eu.texthelp.com/
  https://simplify-us.texthelp.com/
  https://browsealoud-webservices-8.texthelp.com/
  https://browsealoud-webservices-eu.texthelp.com/
  https://babm.texthelp.com
  https://*.speechstream.net
  https://stats.g.doubleclick.net
  https://www.google-analytics.com/
  https://*.google-analytics.com;

 media-src
  'self'
  blob:
  https://*.speechstream.net;
```

Recommended SpeechStream CSP

This is the default CSP that we recommend you use to integrate SpeechStream. Specific parts of this will be explained below.

A CSP can be applied on a page in a meta tag or in a http response header set on the web server. It is up to the website owner to decide the best way to implement their CSP.

This CSP assumes that SpeechStream is loaded with secure protocol (https) and on a secure site and the

website is using the Best Practice SpeechStream Configuration.

Updates to Policy are highlighted in red.

```
default-src
    'self';
  style-src
    'self'
    'unsafe-inline'
    https://*.speechstream.net/
  Script-src
    https://*.speechstream.net
    https://www.googletagmanager.com/
    https://www.google-analytics.com/
    https://apis.google.com
   'sha256-aEDmoObzmjNv962J42VzD3ELW5yetlhKLnYGA32/4aU=';
  img-src
    https://speechstreamv3-webservices-8.texthelp.com/
    https://speechstreamv3-webservices-eu.texthelp.com/
    https://*.speechstream.net
    'self'
    https://*.speechstream.net
    https://www.google-analytics.com/
    https://stats.g.doubleclick.net
    data:;
  child-src
    'self'
    https://content.googleapis.com
    https://www.googletagmanager.com/ns.html;
  Connect-src
    blob:
    https://*.speechstream.net
    https://en.wikipedia.org/
    https://speechstreamv3-webservices-8.texthelp.com/
    https://speechstreamv3-webservices-eu.texthelp.com/
    https://stats.g.doubleclick.net
    https://www.google-analytics.com/;
  media-src
    'self'
    blob:
    https://*.speechstream.net;
```

CSP Explained

Individual parts of the CSP are explained below:

Default-src - This serves as a fallback for the other CSP fetch directives:

- 'Self' - Allow all content hosted on the website's own domain to be loaded

Style-src - Defines valid sources of stylesheets:

- 'Self' - Allow all content hosted on the website's own domain to be loaded`
- 'Unsafe-inline' - The 'unsafe-eval' source expression controls several script execution methods that create code from strings required for the execution of our products

- https://www.browsealoud.com - Loads styles for the ReachDecks user interface
- https://plus.browsealoud.com - Loads styles for the ReachDecks user interface

Script-src - Defines valid sources of JavaScript:

- https://plus.browsealoud.com - Used to allow the main ReachDeck JavaScript to run
- https://www.browsealoud.com - Used to allow the main ReachDeck JavaScript to run
- https://*.speechstream.net - Texthelp domain hosting the speech services including mp3 creation
- https://www.googletagmanager.com - Required to permit Google Tag Manager to run (used to load the Google Analytics Script)
- https://www.google-analytics.com - Required to permit Google Analytics to run (for anonymous usage logging)
- https://apis.google.com - This is required to permit Google Translate to work on your website
- https://wikisum.texthelp.com - This is required to permit the wiki definitions feature in the summariser to run
- 'sha256-aEDmoObzmjNv962J42VzD3ELW5yetlhKLnYGA32/4aU=' - Used to securely inject the Google Tag Manager script on your site, it is a hash of the file being injected to prevent any unknown changes being added

Img-src - This section defines where image files can be loaded from:

- https://browsealoud-webservices-8.texthelp.com/ - Texthelp domain hosting the picture dictionary service for ReachDeck
- https://browsealoud-webservices-eu.texthelp.com/ - Texthelp domain hosting the picture dictionary service for ReachDeck
- https://speechstreamv3-webservices-8.texthelp.com/ - Texthelp domain hosting the picture dictionary service for SpeechStream
- https://speechstreamv3-webservices-eu.texthelp.com/ - Texthelp domain hosting the picture dictionary service for SpeechStream
- self - Allow all content hosted on the website's own domain to be loaded
- https://plus.browsealoud.com - Images loaded as part of the ReachDeck user interface
- https://www.browsealoud.com - Images loaded as part of the ReachDeck user interface
- https://upload.wikimedia.org - This is required to permit the wiki definitions feature to retrieve and display images
- https://www.google-analytics.com - Required for analytics reporting.

- https://stats.g.doubleclick.net - Required for analytics reporting.
- data - Required to allow resources such as Base64 encoded images.
- nd nested browsing contexts loaded using elements such as <frame> and <iframe>:
- 'self' - Allow all content hosted on the website's own domain to be loaded
- https://content.googleapis.com - Required for the Translate feature, which uses Google Translate
- https://www.googletagmanager.com/ns.html - Used to manage our Google Analytics and prevent it clashing with any analytics of your own

Connect-src - Applies to XMLHttpRequest (AJAX), WebSocket or EventSource

- blob: - This is a format that media is returned from the speech servers
- https://plus.browsealoud.com - Used to fetch information files to configure ReachDeck's settings for your website
- https://www.browsealoud.com - Used to allow the main ReachDeck JavaScript to run
- https://en.wikipedia.org - This is required to permit the wiki definitions feature in the summariser to run
- https://wikisum.texthelp.com - This is required to permit the wiki definitions feature in the summariser to run
- https://wiki-summarizer-eu.texthelp.com - This is required to permit the wiki definitions feature in the summariser to run
- https://simplify-us.texthelp.com/ - This is required to use the simplify feature
- https://browsealoud-webservices-8.texthelp.com/ - Texthelp domain hosting the picture dictionary service
- https://browsealoud-webservices-eu.texthelp.com/ - Texthelp domain hosting the picture dictionary service for ReachDeck
- https://babm.texthelp.com - This is where custom pronunciation data is loaded from
- https://*.speechstream.net - Texthelp domain hosting the speech services including mp3 creation

- https://stats.g.doubleclick.net - Used for ReachDeck usage analytics.
- https://www.google-analytics.com - Used for our products usage analytics.
- https://*.google-analytics.com - Used for ReachDeck usage analytics (GA4). The * is a wildcard that will allow google-analytics.com to be accessed from any region.

Media-src - This defines where media files are permitted to be loaded from

- blob - This is a format that media is returned from the speech servers
- 'self' - Allow all content hosted on the website's own domain to be loaded
- https://*.speechstream.net - Texthelp domain hosting the speech services including mp3 creation