
Header Content-Security-Policy - block carousel

Posted by ZAJDAN - 2016/09/06 08:40

Hello,
on my server I am setting a few new security rules and one thing makes me problem with carousel.
When I set on appache server:
Header add Content-Security-Policy "default-src 'self'"
the carousel has problem to load

Thank You for any hint
Regards ZAJDAN

Re:Header Content-Security-Policy - block carousel

Posted by admin - 2016/09/06 10:04

Hello,

Where we can see the problem?

Regards,
ARI Soft

Re:Header Content-Security-Policy - block carousel

Posted by ZAJDAN - 2016/09/06 10:22

when I enable the rule on apache, then I look on the web via Inspect...there I see:

Refused to apply inline style because it violates the following Content Security Policy directive: "default-src 'self'". Either the 'unsafe-inline' keyword, a hash ('sha256-d5IFtN8ELvhf7ulae/5+laak+QG9Sf0hVaQThwHzk8U='), or a nonce ('nonce-...') is required to enable inline execution. Note also that 'style-src' was not explicitly set, so 'default-src' is used as a fallback.

konfigurator:1 Refused to load the script 'http://ajax.googleapis.com/ajax/libs/jquery/1.4.4/jquery.min.js' because it violates the following Content Security Policy directive: "default-src 'self'". Note that 'script-src' was not explicitly set, so 'default-src' is used as a fallback.

jquery.cloud-carousel.min.js
Uncaught EvalError: Refused to evaluate a string as JavaScript because 'unsafe-eval' is not an allowed source of script in the following Content Security Policy directive: "default-src 'self'". konfigurator:73 Refused to execute inline script because it violates the following Content Security Policy directive: "default-src 'self'". Either the 'unsafe-inline' keyword, a hash ('sha256-GAT6NNfoBUzoYAQ5fVBCycaDZg+q7QqsnmWB/0f2NHk='), or a nonce ('nonce-...') is required to enable inline execution. Note also that 'script-src' was not explicitly set, so 'default-src' is used as a fallback.

Re:Header Content-Security-Policy - block carousel

Posted by admin - 2016/09/06 10:28

jquery.cloud-carousel.min.js is minified version of javascript file and it is used "eval" javascript function. It is a normal for minifier applications.

About ajax.googleapis.com/ajax/libs/jquery/1.4.4/jquery.min.js file, it loads from Google CDN. If you use Joomla! 3+, the extension will load jQuery via Joomla! API from your server. Just set "Load jQuery method" parameter to "Local copy".

Regards,
ARI Soft

=====

Re:Header Content-Security-Policy - block carousel

Posted by ZAJDAN - 2016/09/07 07:47

I use older Joomla 2.5
this library is called from cloud carousel?:
ajax.googleapis.com/ajax/libs/jquery/1.4.4/jquery.min.js

because I manually call just jquery 2.4

Thank You

Regards ZAJDAN

=====

Re:Header Content-Security-Policy - block carousel

Posted by admin - 2016/09/07 11:46

You can disable loading of jQuery library in module settings if it is loaded by site template or a 3rd party extension.

Regards,
ARI Soft

=====