

ISTI Open Access - Support #16178

Joomla Security Update

Feb 27, 2019 12:46 PM - Michele Artini

Status:	Closed	Start date:	Feb 27, 2019
Priority:	Normal	Due date:	
Assignee:	Andrea Dell'Amico	% Done:	100%
Target version:	ISTI Open Portal Issues		
VREName:			
Description			
Message after the last Joomla update:			
<code>.htaccess & web.config security Update</code> <code>Since version 3.9.3</code>			
<code>Since Joomla 3.9.3, Joomla is shipped with additional security hardenings in the default htaccess.txt and web.config.txt files.</code> <code>These hardenings disable the so called MIME-type sniffing feature in webbrowsers. The sniffing leads to specific attack vectors,</code> <code>where scripts in normally harmless file formats (i.e. images) will be executed, leading to Cross-Site-Scripting vulnerabilities.</code>			
<code>The security teams recommends to manually apply the necessary changes to existing .htaccess or web.config files,</code> <code>as those files can not be updated automatically.</code>			
<code>Changes for .htaccess</code> <code>Add the following lines before "## Mod_rewrite in use.":</code>			
<code><IfModule mod_headers.c></code> <code>Header always set X-Content-Type-Options "nosniff"</code> <code></IfModule></code>			
<code>Changes for web.config</code> <code>Add the following lines right after "</rewrite>":</code>			
<code><httpProtocol></code> <code><customHeaders></code> <code><add name="X-Content-Type-Options" value="nosniff" /></code> <code></customHeaders></code> <code></httpProtocol></code>			

History

#1 - Feb 27, 2019 01:17 PM - Andrea Dell'Amico

- Status changed from New to In Progress

#2 - Feb 27, 2019 01:23 PM - Andrea Dell'Amico

- Status changed from In Progress to Feedback

- % Done changed from 0 to 100

Done. The second configuration entry cannot be applied to our apache server, it works with apache versions newer that the one we run.

#3 - Feb 27, 2019 02:37 PM - Andrea Dell'Amico

- Status changed from Feedback to Closed