

Redmine - Defect #30255

This site can't provide a secure connection www.redmine.org uses an unsupported protocol.
ERR_SSL_VERSION_OR_CIPHER_MISMATCH

2018-12-20 09:41 - Anatolii Vorona

Status:	Closed	Start date:	
Priority:	Normal	Due date:	
Assignee:	Jean-Philippe Lang	% Done:	0%
Category:	Website (redmine.org)	Estimated time:	0.00 hour
Target version:		Affected version:	
Resolution:	Fixed		
Description			
I'm using chrome with option --ssl-version-min=tls1.2 And can't access to https://www.redmine.org/ The vulnerabilities within SSL and early TLS are serious. Please update your SSL/TLS configuration. !Screenshot from 2018-12-20 09-32-46.png! !Screenshot from 2018-12-20 09-32-20.png! I recommend you to check result with this link https://www.ssllabs.com/ssltest/analyze.html?d=www.redmine.org			

History

#1 - 2018-12-20 10:02 - Go MAEDA

The server must be updated in a hurry. TLS 1.1 support will be dropped by 2020 in most web browsers.

<https://blog.mozilla.org/security/2018/10/15/removing-old-versions-of-tls/>
<https://security.googleblog.com/2018/10/modernizing-transport-security.html>
<https://blogs.windows.com/msedgedev/2018/10/15/modernizing-tls-edge-ie11/>
<https://webkit.org/blog/8462/deprecation-of-legacy-tls-1-0-and-1-1-versions/>

#2 - 2018-12-20 16:53 - Bernhard Rohloff

The Qualys rating is really awful!
[jp.jp](#) If we can help you in any kind of way don't feel afraid to ask. :-)

#3 - 2018-12-20 17:04 - Anatolii Vorona

by the way
<https://mozilla.github.io/server-side-tls/ssl-config-generator/>

#4 - 2019-01-19 06:28 - Franklin Yu

There has been an issue [#29202](#), but it was marked as duplicate of an internal issue.

#6 - 2019-10-07 19:27 - Jan Niggemann (redmine.org team member)

[jp.jp](#): We have 6 months before TLS 1.1 support is dropped. How can we assist you / what can we do to get the server updated?

#7 - 2020-01-10 03:22 - Go MAEDA

- Status changed from New to Closed

- Resolution set to Fixed

www.redmine.org now supports TLS 1.2.

```
$ curl --tlsv1.2 --head https://www.redmine.org/  
HTTP/1.1 200 OK  
Date: Fri, 10 Jan 2020 02:15:59 GMT  
Server: Apache  
X-UA-Compatible: IE=Edge,chrome=1  
.  
.  
.
```

Files

Screenshot from 2018-12-20 09-32-20.png	37.8 KB	2018-12-20	Anatolii Vorona
Screenshot from 2018-12-20 09-32-46.png	106 KB	2018-12-20	Anatolii Vorona