

Ruby - Bug #14204

[PATCH] socket: use frozen string buffer when releasing GVL

12/19/2017 07:49 AM - normalperson (Eric Wong)

Status:	Closed	
Priority:	Normal	
Assignee:	akr (Akira Tanaka)	
Target version:		
ruby -v:		
Backport:		2.3: UNKNOWN, 2.4: UNKNOWN
Description		
<code>socket: use frozen string buffer when releasing GVL</code>		
Using a non-frozen string buffer when GVL is released is dangerous because another thread may modify that buffer. This may lead to the contents of an invalid pointer being written to the socket.		
Follow the lead used with core io.c methods and duplicate the string to a temporary frozen buffer before writing.		
<pre>* ext/socket/ancdata.c (bsock_sendmsg_internal): use rb_str_tmp_frozen_{acquire/release} as with IO#write * internal.h (rb_str_tmp_frozen_acquire): export (rb_str_tmp_frozen_release): export</pre>		
related to [Bug #14195]		

Associated revisions

Revision 4900a10689036211da79c8189ff7eba11c8c81ee - 07/14/2019 11:46 AM - akr (Akira Tanaka)

socket: use frozen string buffer when releasing GVL

Thanks for the patch by normalperson (Eric Wong) [Bug #14204].

Revision 4900a10689036211da79c8189ff7eba11c8c81ee - 07/14/2019 11:46 AM - akr (Akira Tanaka)

socket: use frozen string buffer when releasing GVL

Thanks for the patch by normalperson (Eric Wong) [Bug #14204].

Revision 4900a106 - 07/14/2019 11:46 AM - akr (Akira Tanaka)

socket: use frozen string buffer when releasing GVL

Thanks for the patch by normalperson (Eric Wong) [Bug #14204].

History

#1 - 07/14/2019 11:49 AM - akr (Akira Tanaka)

- Status changed from Open to Closed

Applied in changeset [git|4900a10689036211da79c8189ff7eba11c8c81ee](#).

socket: use frozen string buffer when releasing GVL

Thanks for the patch by normalperson (Eric Wong) [Bug #14204].

Files

0001-socket-use-frozen-string-buffer-when-releasing-GVL.patch	3.03 KB	12/19/2017	normalperson (Eric Wong)
---	---------	------------	--------------------------