Ruby master - Bug #5647

Possible use of uninitialized value in Init_bigdecimal

11/18/2011 05:52 PM - brixen (Brian Shirai)

Status:	Closed		
Priority:	Normal		
Assignee:	mrkn (Kenta Murata)		
Target version:			
ruby -v:	ruby 1.9.3p0 (2011-10-30 revision 33570) [x86_64-darwin10.8.0]	**Backport:**	

Description

I see the following call chain in bigdecimal.c

Init_bigdecimal -> VpInit -> VpAlloc -> VpGetPrecLimit -> rb_thread_local_aref with id_BigDecimal_precision_limit

The call to VpInit occurs before the call to set the value of id_BigDecimal_precision_limit in Init_bigdecimal.

So it appears that a thread local is set with the key of an uninitialized C value, if I'm following correctly.

Thanks,
Brian

Related issues:

Has duplicate Ruby master - Bug #6406: Ruby crashes with Segmentation fault	**Closed**	**05/06/2012**

History

#1 - 03/11/2012 04:49 PM - mrkn (Kenta Murata)

- Assignee set to mrkn (Kenta Murata)

#2 - 03/18/2012 06:46 PM - shyouhei (Shyouhei Urabe)

- Status changed from Open to Assigned

#3 - 06/01/2012 11:45 AM - mrkn (Kenta Murata)

- Status changed from Assigned to Closed

This is fixed by r35555