Ruby - Bug #20718

Objects created with Data_Make_Struct and the default free function are not freed

09/06/2024 09:45 PM - jcalvert (Jonathan Calvert)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:	ruby 3.3.5 (2024-09-03 revision ef084cc8f4) [x86_64-linux]	**Backport:**	3.1: DONTNEED, 3.2: DONTNEED, 3.3: DONE

Description

I discovered a memory leak when using the FFI gem prior to version 1.16 and Ruby 3.3 and up.

During debugging I found that this earlier version of FFI uses Data_Make_Struct (https://github.com/ffi/ffi/blob/v1.15.5/ext/ffi_c/Pointer.c#L57) instead of TypedData_Make_Struct and it uses -1 as the free function, which is RUBY_DEFAULT_FREE

When the object goes to get garbage collected, it enters into rb_data_free and it is passed to the RTYPEDDATA_EMBEDDED_P macro even though it is not of RTypedData. Because of that, the conditional is evaluated to false and xfree is never called. This was discovered by using jemalloc leak detection.

I have attached a somewhat minimal replication of the issue. The fix would appear to check the type of the obj before casting it.

Associated revisions

Revision c1a510a8dffa1c8065e47697cd57edae67126712 - 09/07/2024 03:19 AM - jcalvert (Jonathan Calvert)

[Bug #20718] Free non-RTypedData objects

Allow objects that are not of type RTypedData to use the default
free function, as RTYPEDDATA_EMBEDDED_P can return a false positive
when casting non-RTypedData objects.

Revision c1a510a8dffa1c8065e47697cd57edae67126712 - 09/07/2024 03:19 AM - jcalvert (Jonathan Calvert)

[Bug #20718] Free non-RTypedData objects

Allow objects that are not of type RTypedData to use the default
free function, as RTYPEDDATA_EMBEDDED_P can return a false positive
when casting non-RTypedData objects.

Revision c1a510a8 - 09/07/2024 03:19 AM - jcalvert (Jonathan Calvert)

[Bug #20718] Free non-RTypedData objects

Allow objects that are not of type RTypedData to use the default
free function, as RTYPEDDATA_EMBEDDED_P can return a false positive
when casting non-RTypedData objects.

Revision 55ddfd58dd6e67e88cf9a3e55bf99550affe8b3f - 09/11/2024 12:38 AM - jcalvert (Jonathan Calvert)

Fixes [Bug #20718] (#11576)

Fixes [Bug #20718]

Allow objects that are not of type RTypedData to use the default free function, as RTYPEDDATA_EMBEDDED_P can return a false positive when casting non-RTypedData objects

Revision 55ddfd58dd6e67e88cf9a3e55bf99550affe8b3f - 09/11/2024 12:38 AM - jcalvert (Jonathan Calvert)

Fixes [Bug #20718] (#11576)

Fixes [Bug #20718]

Allow objects that are not of type RTypedData to use the default free function, as RTYPEDDATA_EMBEDDED_P can return a false positive when casting non-RTypedData objects

Revision 55ddfd58 - 09/11/2024 12:38 AM - jcalvert (Jonathan Calvert)

Fixes [Bug #20718] (#11576)

Fixes [Bug #20718]

Allow objects that are not of type RTypedData to use the default free function, as RTYPEDDATA_EMBEDDED_P can return a false positive when casting non-RTypedData objects

History

#1 - 09/06/2024 09:55 PM - jcalvert (Jonathan Calvert)

I have added a pull request that should patch the issue. https://github.com/ruby/ruby/pull/11563 - I was able to build Ruby and run it against my example and it does work.

Presumably this would be a candidate for a backport :)

#2 - 09/07/2024 03:19 AM - jcalvert (Jonathan Calvert)

- Status changed from Open to Closed

Applied in changeset git|c1a510a8dffa1c8065e47697cd57edae67126712.

[Bug #20718] Free non-RTypedData objects

Allow objects that are not of type RTypedData to use the default
free function, as RTYPEDDATA_EMBEDDED_P can return a false positive
when casting non-RTypedData objects.

#3 - 09/07/2024 05:00 PM - byroot (Jean Boussier)

- Backport changed from 3.1: UNKNOWN, 3.2: UNKNOWN, 3.3: UNKNOWN to 3.1: DONTNEED, 3.2: DONTNEED, 3.3: REQUIRED

I think this issue was introduced in 3.3? Let me know if not and I'll update the backport target.

Also for 3.3 the branch maintainer appreciate backport PRs so don't hesitate to open it yourself and tag k0kubun if you wish.

#4 - 11/04/2024 10:18 PM - k0kubun (Takashi Kokubun)

- Backport changed from 3.1: DONTNEED, 3.2: DONTNEED, 3.3: REQUIRED to 3.1: DONTNEED, 3.2: DONTNEED, 3.3: DONE

ruby_3_3 55ddfd58dd6e67e88cf9a3e55bf99550affe8b3f.

Files

pointer_bug.rb	418 Bytes	09/06/2024	jcalvert (Jonathan Calvert)
Gemfile.txt	104 Bytes	09/06/2024	jcalvert (Jonathan Calvert)