Bug 105039 - rust demangler stack overflow

Status:	RESOLVED FIXED	**Reported:**	2022-03-24 00:33 UTC by Alan Modra
Alias:	None	**Modified:**	2022-07-04 03:50 UTC (History)
		CC List:	5 users (show)
Product:	gcc		
Component:	demangler (show other bugs)	**See Also:**	
Version:	12.0	**Host:**	
		Target:	
Importance:	P3 normal	**Build:**	
Target Milestone:	---	**Known to work:**	
Assignee:	Not yet assigned to anyone	**Known to fail:**	
		Last reconfirmed:	
URL:			
Keywords:			
Depends on:			
Blocks:			

Attachments

Add an attachment (proposed patch, testcase, etc.)

Note

You need to log in before you can comment on or make changes to this bug.

Alan Modra **2022-03-24 00:33:20 UTC** **Description**

From https://sourceware.org/bugzilla/show_bug.cgi?id=28995

```
c++filt _RYAaca_NRYAaBa_a

AddressSanitizer:DEADLYSIGNAL
=================================================================
==4145846==ERROR: AddressSanitizer: stack-overflow on address 0x7ffd205e8ff8 (pc
0x0000021dfea9 bp 0x00000000005f sp 0x7ffd205e9000 T0)
    #0 0x21dfea9 in peek /home/alan/src/binutils-gdb/libiberty/rust-demangle.c:90
    #1 0x21dfd8c in eat /home/alan/src/binutils-gdb/libiberty/rust-demangle.c:99:7
    #2 0x21e1bb4 in parse_integer_62 /home/alan/src/binutils-gdb/libiberty/rust-
demangle.c:125:7
    #3 0x21e2019 in demangle_const /home/alan/src/binutils-gdb/libiberty/rust-
demangle.c:1153:17
    #4 0x21e20a7 in demangle_const /home/alan/src/binutils-gdb/libiberty/rust-
demangle.c:1158:11

and lots more at 1158:11.  This is with libiberty sources from gcc commit
4cebae0924248b.
```

Nick Clifton **2022-03-24 13:13:59 UTC** **Comment 1**

Proposed patch submitted here:

https://gcc.gnu.org/pipermail/gcc-patches/2022-March/592244.html

Jeremy Robinson 2022-05-12 22:59:31 UTC **Comment 2**

Respectfully pinging this issue to ask for a review of the proposed patch.

hs.naveen2u 2022-06-27 09:54:27 UTC **Comment 3**

Can anyone please review the patch so that it can be used?

CVS Commits 2022-07-01 15:00:27 UTC **Comment 4**

The master branch has been updated by Nick Clifton <nickc@gcc.gnu.org>:

https://gcc.gnu.org/g:9234cdca6ee88badfc00297e72f13dac4e540c79

commit r13-1393-g9234cdca6ee88badfc00297e72f13dac4e540c79
Author: Nick Clifton <nickc@redhat.com>
Date: Fri Jul 1 15:58:52 2022 +0100

Add a recursion limit to the demangle_const function in the Rust demangler.

libiberty/
~~PR demangler/105039~~
* rust-demangle.c (demangle_const): Add recursion limit.

Nick Clifton 2022-07-01 15:01:22 UTC **Comment 5**

Patch applied.

hs.naveen2u 2022-07-04 03:50:50 UTC **Comment 6**

Thanks very much for committing the patch.