SEGV on _IO_str_init_static_internal()

A portable, multi-platform, command-line driven graphing utility

Brought to you by: broeker, cgaylord, lhecking, sfeam

#2781 SEGV on _IO_str_init_static_internal()

Milestone: None	**Status:** closed-fixed	**Owner:** nobody	**Labels:** None
Priority:			
Updated: 2025-09-14	**Created:** 2025-03-25	**Creator:** liuchenyifan	**Private:** No

version: gnuplot 6.1 last modified 2025-03-05
system: ubuntu 22.04

use this command to reproduce: valgrind gnutplot poc
message from valgrind:

```
==3801983== Memcheck, a memory error detector
==3801983== Copyright (C) 2002-2017, and GNU GPL'd, by Julian Seward et al.
==3801983== Using Valgrind-3.18.1 and LibVEX; rerun with -h for copyright info
==3801983== Command: ./gnuplot ./bugs/SEGV__IO_str_init_static_internal
==3801983==
Warning: empty x range [0:0], adjusting to [-1:1]
Warning: empty y range [1:1], adjusting to [0.99:1.01]
==3801983== Invalid read of size 1
==3801983== at 0x4853369: rawmemchr (in /usr/libexec/valgrind/vgpreload_memcheck-amd64-linux.so)
==3801983== by 0x4D3C9E7: _IO_str_init_static_internal (strops.c:41)
==3801983== by 0x4D0F322: _IO_strfile_read (strfile.h:95)
==3801983== by 0x4D0F322: __isoc99_sscanf (isoc99_sscanf.c:28)
==3801983== by 0x52296A: HPGL2_set_font (hpgl.trm:1672)
==3801983== by 0x5747F8: write_multiline (term.c:786)
==3801983== by 0x27B274: ytick2d_callback (graphics.c:4280)
==3801983== by 0x13E7A6: gen_tics (axis.c:1412)
==3801983== by 0x141B42: axis_output_tics (axis.c:1744)
==3801983== by 0x26FD22: place_grid (graphics.c:223)
==3801983== by 0x2BF608: do_plot (graphics.c:777)
==3801983== by 0x38A74A: eval_plots (plot2d.c:4136)
==3801983== by 0x1705CB: plot_command (command.c:2174)
==3801983== Address 0x586230c is 0 bytes after a block of size 12 alloc'd
==3801983== at 0x4848899: malloc (in /usr/libexec/valgrind/vgpreload_memcheck-amd64-linux.so)
==3801983== by 0x4D5558E: strdup (strdup.c:42)
==3801983== by 0x1DAC10: push (eval.c:665)
==3801983== by 0x1DB10D: execute_at (eval.c:767)
==3801983== by 0x1DB10D: evaluate_at (eval.c:802)
==3801983== by 0x37319E: const_express (parse.c:175)
==3801983== by 0x37319E: const_string_express (parse.c:153)
==3801983== by 0x59FF47: try_to_get_string (util.c:378)
==3801983== by 0x438017: set_tic_prop (set.c:5644)
==3801983== by 0x44FFF5: set_tics (set.c:5095)
==3801983== by 0x44FFF5: set_command (set.c:497)
==3801983== by 0x16A6E5: command (command.c:855)
==3801983== by 0x16A6E5: step_through_line (command.c:549)
==3801983== by 0x338037: load_file (misc.c:393)
==3801983== by 0x123AE4: main (plot.c:669)
==3801983==
"./bugs/SEGV__IO_str_init_static_internal" line 18: warning: Bad data on line 1 of file -
"./bugs/SEGV__IO_str_init_static_internal" line 19: warning: Bad data on line 2 of file -
"./bugs/SEGV__IO_str_init_static_internal" line 23: warning: Bad data on line 6 of file -
"./bugs/SEGV__IO_str_init_static_internal" line 24: warning: Bad data on line 7 of file -
"./bugs/SEGV__IO_str_init_static_internal" line 25: warning: Bad data on line 8 of file -
"./bugs/SEGV__IO_str_init_static_internal" line 26: warning: Bad data on line 9 of file -
```

```
Warning: empty x range [0:0], adjusting to [-1:1]
Warning: empty y range [0:0], adjusting to [-1:1]
Warning: empty z range [0:0], adjusting to [-1:1]
==3801983== Invalid read of size 8
==3801983== at 0x23DFA9: plot3d_points (graph3d.c:2167)
==3801983== by 0x260B8B: do_3dplot (graph3d.c:1242)
==3801983== by 0x3B66DD: eval_3dplots (plot3d.c:3057)
==3801983== by 0x173B1D: splot_command (command.c:2749)
==3801983== by 0x16A6E5: command (command.c:855)
==3801983== by 0x16A6E5: step_through_line (command.c:549)
==3801983== by 0x338037: load_file (misc.c:393)
==3801983== by 0x123AE4: main (plot.c:669)
==3801983== Address 0x50 is not stack'd, malloc'd or (recently) free'd
==3801983==
==3801983==
==3801983== Process terminating with default action of signal 11 (SIGSEGV)
==3801983== Access not within mapped region at address 0x50
==3801983== at 0x23DFA9: plot3d_points (graph3d.c:2167)
==3801983== by 0x260B8B: do_3dplot (graph3d.c:1242)
==3801983== by 0x3B66DD: eval_3dplots (plot3d.c:3057)
==3801983== by 0x173B1D: splot_command (command.c:2749)
==3801983== by 0x16A6E5: command (command.c:855)
==3801983== by 0x16A6E5: step_through_line (command.c:549)
==3801983== by 0x338037: load_file (misc.c:393)
==3801983== by 0x123AE4: main (plot.c:669)
==3801983== If you believe this happened as a result of a stack
==3801983== overflow in your program's main thread (unlikely but
==3801983== possible), you can try to increase the size of the
==3801983== main thread stack using the --main-stacksize= flag.
==3801983== The main thread stack size used in this run was 8388608.
==3801983==
==3801983== HEAP SUMMARY:
==3801983== in use at exit: 117,056 bytes in 612 blocks
==3801983== total heap usage: 840 allocs, 228 frees, 364,889 bytes allocated
==3801983==
==3801983== LEAK SUMMARY:
==3801983== definitely lost: 0 bytes in 0 blocks
==3801983== indirectly lost: 0 bytes in 0 blocks
==3801983== possibly lost: 0 bytes in 0 blocks
==3801983== still reachable: 115,040 bytes in 591 blocks
==3801983== suppressed: 0 bytes in 0 blocks
==3801983== Rerun with --leak-check=full to see details of leaked memory
==3801983==
==3801983== For lists of detected and suppressed errors, rerun with: -s
==3801983== ERROR SUMMARY: 15 errors from 2 contexts (suppressed: 0 from 0)
Segmentation fault
```

1 Attachments

SEGV _IO_str_init_static_internal

Discussion

Ethan Merritt - *2025-03-27*

- **status**: open --> closed-fixed
- **Group**: -->
- **Priority**: -->

Orion Poplawski - *2025-09-13*

What commit fixed this? It seems like this was assigned CVE-2025-3359 so it would be nice to have a reference

MongoDB.

Orion Poplawski - *2025-09-13*

Ah - looks like this: a5897feadc4be73b0ffd8458556c47117bd24d03

hpgl: font name parsing overruns the string by one char

```
if no comma is present in the font name.
E.g.
   set term pcl
   set title "Title" font "sans"    # no comma in font name
   plot x

Bug 2781
```

Orion Poplawski - *2025-09-13*

Any ETA on a new release with this fix? Thanks.

Ethan Merritt - *2025-09-13*

The fix used for 6.1 does not apply cleanly to the stable branch. Given that the bug had been in the code for decades with no reported problems, it did not seem worth the effort to back-port or work out a different fix for 6.0.

Is this issue causing you a problem in current stable (6.0.3)?

Orion Poplawski - *2025-09-13*

Not particularly. I'm just going through various bug reports on gnuplot in Fedora and came across the CVE report related to this crash.

Ethan Merritt - *2025-09-14*

OK. I'll look to see what the glitch is with cherry-picking the 6.1 fix, and queue it for 6.0.4

Log in to post a comment.

SourceForge

Create a Project
Open Source Software
Business Software
Top Downloaded Projects

Company

About
Team
SourceForge Headquarters
1320 Columbia Street Suite 310
San Diego, CA 92101
+1 (858) 422-6466

Resources

Support
Site Documentation
Site Status
SourceForge Reviews

MongoDB.

© 2026 Slashdot Media. All Rights Reserved.

Your Opt-Out Rights Cookie Choices
Terms Privacy Advertise