Re: [Bug-gama] [bug report] NULL-pointer deference in GNU_gama::set() in

From: Aleš Čepek
Subject: Re: [Bug-gama] [bug report] NULL-pointer deference in GNU_gama::set() in ellipsoid.h
Date: Sun, 7 Apr 2019 17:11:51 +0200

Fixed in gama-2.04 (next version).
ac

On Tue, 2 Apr 2019 at 14:01, wcventure <address@hidden> wrote:

> Hi there,
>
> I have found NULL-pointer deference in GNU_gama::set() in ellipsoid.h, in gama 2.04 the lastest release version. A crafted input can cause segment faults and I have confirmed them with address sanitizer too.
>
> Here are the POC files. Please use the "./gama-g3 --algorithm envelope $POC ./tmp" to reproduce the bug.
>
> The ASAN dumps the stack trace as follows:

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==188911==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000028 (pc 0x0000006d4c19 bp 0x7ffe67787e50 sp 0x7ffe67787b70 T0)
==188911==The signal is caused by a WRITE memory access.
==188911==Hint: address points to the zero page.
    #0 0x6d4c18 in GNU_gama::set(GNU_gama::Ellipsoid*, GNU_gama::gama_ellipsoid) /gama-2.04/lib/./gnu_gama/ellipsoid.h:45:42
    #1 0x63b53e in GNU_gama::DataParser::g3_const_ellipsoid_b(char const*) /gama-2.04/lib/gnu_gama/xml/dataparser_g3.cpp:1223:6
    #2 0x7fb90df723ea in _init (/lib/x86_64-linux-gnu/libexpat.so.1+0x83ea)
    #3 0x7fb90df733ab in _init (/lib/x86_64-linux-gnu/libexpat.so.1+0x93ab)
    #4 0x7fb90df74ccd in _init (/lib/x86_64-linux-gnu/libexpat.so.1+0xaccd)
    #5 0x7fb90df75424 in _init (/lib/x86_64-linux-gnu/libexpat.so.1+0xb424)
    #6 0x7fb90df7772a in XML_ParseBuffer (/lib/x86_64-linux-gnu/libexpat.so.1+0xd72a)
    #7 0x51ff33 in GNU_gama::BaseParser<GNU_gama::Exception::parser>::xml_parse(char const*, int, int) /gama-2.04/bin/../lib/gnu_gama/xml/baseparser.h:84:17
    #8 0x51a340 in main_g3() /gama-2.04/bin/gama-g3.cpp:141:20
    #9 0x51d64d in main /gama-2.04/bin/gama-g3.cpp:231:14
    #10 0x7fb90ccea82f in __libc_start_main /build/glibc-Cl5G7W/glibc-2.23/csu/../csu/libc-start.c:291
    #11 0x41d2b8 in _start (/gama-2.04/build/bin/gama-g3+0x41d2b8)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /gama-2.04/lib/./gnu_gama/ellipsoid.h:45:42 in GNU_gama::set(GNU_gama::Ellipsoid*, GNU_gama::gama_ellipsoid)
==188911==ABORTING
```

> Thanks

> _____
> Bug-gama mailing list
> address@hidden
> https://lists.gnu.org/mailman/listinfo/bug-gama

reply via email to
Aleš Čepek

[Prev in Thread] **Current Thread** [Next in Thread]

- **[Bug-gama] [bug report] NULL-pointer deference in GNU_gama::set() in ellipsoid.h**, *wcventure*, 2019/04/02
  - **Re: [Bug-gama] [bug report] NULL-pointer deference in GNU_gama::set() in ellipsoid.h**, *Aleš Čepek* <=
    - **[Bug-gama] 2.04 release**, *Greg Troxel*, 2019/04/08

- Prev by Date: **[Bug-gama] [bug report] NULL-pointer deference in GNU_gama::set() in ellipsoid.h**
- Next by Date: **[Bug-gama] 2.04 release**
- Previous by thread: **[Bug-gama] [bug report] NULL-pointer deference in GNU_gama::set() in ellipsoid.h**
- Next by thread: **[Bug-gama] 2.04 release**
- Index(es):
  - **Date**
  - **Thread**