RADOS - Bug #38296

segv in fgets() in collect_sys_info reading /proc/cpuinfo

02/13/2019 12:59 PM - Sage Weil

Status: Resolved
Priority: High
Assignee:
Category:
Target version:
Source:
Tags: nautilus, mimic, luminous
Backport: n/a
Regression: No
Severity: 3 - minor
Reviewed:

Affected Versions:
Component(RADOS):
Pull request ID: 27707

Crash signature (v1):
Crash signature (v2):

Description

#0 raise (sig=sig@entry=11) at ../sysdeps/unix/sysv/linux/raise.c:51
#1 0x00005645a29f47a3 in reraise_fatal (signum=11) at ./src/global/signal_handler.cc:81
#2 handle_fatal_signal (signum=11) at ./src/global/signal_handler.cc:298
#3 <signal handler called>
#4 __memchr_avx2 () at ../sysdeps/x86_64/multiarch/memchr-avx2.S:92
#5 0x00007fe855e9f2d0 in __GI__IO_getline_info (eof=0x0, extract_delim=<optimized out>, delim=10, n=99, buf=0x7fe855e9f2d0 "DirectMap1G: 31457280 kB\n", fp=0x5645a3c7dcc0, fp@entry=0x1) at iogetline.c:85
#6 __GI__IO_getline (fp=fp@entry=0x5645a3c7dcc0, buf=buf@entry=0x7fe855e9f2d0 "DirectMap1G: 31457280 kB\n", n=n@entry=99, delim=delim@entry=10, extract_delim=extract_delim@entry=1) at iogetline.c:34
#7 0x00007fe8616a5bdc in __IO_fgets (buf=buf@entry=0x7fe855e9f2d0 "DirectMap1G: 31457280 kB\n", n=n@entry=100, fp=fp@entry=0x5645a3c7dcc0) at iofgets.c:53
#8 0x00007fe863b3a930 in fgets (__stream=0x5645a3c7dcc0, __n=100, __s=0x7fe855e9f2d0 "DirectMap1G: 31457280 kB\n") at /usr/include/x86_64-linux-gnu/bits/stdio2.h:262
#9 collect_sys_info (m=m@entry=0x5645a3c86348, cct=<optimized out>) at ./src/common/util.cc:232
#10 0x00005645a278465b in Monitor::collect_metadata (this=this@entry=0x5645a505b400, m=0x5645a3c86348) at ./src/Monitor.cc:2220
#11 0x00005645a2827227 in Elector::start (this>this@entry=0x5645a505c0f0) at ./src/Elector.cc:99
#12 0x00005645a2796221 in Elector::call_election (this=0x5645a505c0f0) at ./src/Elector.cc:387
#13 0x00005645a27826b17 in Elector::handle_propose (this=0x5645a505c0f0, op=...) at ./src/Elector.cc:287
#14 0x00005645a28286e9 in Elector::dispatch (this=0x5645a505c0f0, op=...) at ./src/Elector.cc:509
#15 0x00005645a27afba8 in Monitor::dispatch_op (this=this@entry=0x5645a505b400, op=...) at ./src/Monitor.cc:4468
#16 0x00005645a27b05c2 in Monitor::_ms_dispatch (this=0x5645a505b400, m=m@entry=0x5645ccfadcd0) at ./src/Monitor.cc:4261
#17 0x00005645a27dd703 in Monitor::ms_dispatch (this=0x5645a505b400, m=0x5645ccfadcd0) at ./src/Monitor.cc:287
#18 0x00005645a27d9e26 in Dispatcher::ms_dispatch2 (this=0x5645a505b400, m=...) at ./src/msg/Dispatcher.cc:126
#19 0x00005645a27d9e26 in Dispatcher::ms_dispatch2 (this=0x5645a505b400, m=...) at ./src/msg/Dispatcher.cc:126
#20 0x00005645a4f800 in Messenger::ms_deliver_dispatch (m=..., this=0x5645a4f800) at ./src/msg/Messenger.cc:647
#21 DispatchQueue::entry (this=0x5645a4f800) at ./src/msg/DispatchQueue.cc:196

/a/sage-2019-02-13_03:03:14:34-upgrade:luminous-x-wip-v2-upgrade-distro-basic-smithi/3582464
the line in question is

```c
char *line = fgets(buf, sizeof(buf), f);
```

```c
f = fopen(PROCPREFIX "*/proc/cpuinfo", "r");
if (f) {
    char buf[1024];
    while (!feof(f)) {
        char *line = fgets(buf, sizeof(buf), f);
        if (!line)
            break;
        if (strcmp(line, "model name") == 0) {
            char *c = strchr(buf, ':');
            c++;
            while (*c == ' ')
                ++c;
            char *nl = c;
            while (*nl != '\n')
                ++nl;
            *nl = '\0';
            (*m)["cpu"] = c;
            break;
        }
    }
    fclose(f);
}
```

Related issues:

- Related to RADOS - Bug #43306: segv in collect_sys_info
  Resolved
- Copied to RADOS - Backport #39474: luminous: segv in fgets() in collect_sys_info...
  Resolved
- Copied to RADOS - Backport #39475: mimic: segv in fgets() in collect_sys_info...
  Resolved
- Copied to RADOS - Backport #39476: nautilus: segv in fgets() in collect_sys_info...
  Resolved

History:

#1 - 04/22/2019 05:48 PM - Sage Weil

- Priority changed from Normal to High

saw this again:

```
2019-04-17T23:51:44.683 INFO:tasks.ceph.mon.a.smithi002.stderr: 3: (_IO_getline()+0x55) [0x7febc8dd5e25]
2019-04-17T23:51:44.683 INFO:tasks.ceph.mon.a.smithi002.stderr: 4: (fgets()+0xad) [0x7febc8dd4bcd]
2019-04-17T23:51:44.684 INFO:tasks.ceph.mon.a.smithi002.stderr: 5: (collect_sys_info(std::map<std::basic_string<char, std::char_traits<char>, std::allocator<char> >, std::basic_string<char, std::char_traits<char>, std::allocator<char> >, std::less<std::basic_string<char, std::char_traits<char>, std::allocator<char> > >, std::allocator<std::pair<std::basic_string<char, std::char_traits<char>, std::allocator<char> > const, std::basic_string<char, std::char_traits<char>, std::allocator<char> > > >, std::allocator<char> >, std::less<std::basic_string<char, std::char_traits<char>, std::allocator<char> > >, std::pair<std::basic_string<char, std::char_traits<char>, std::allocator<char> > const, std::basic_string<char, std::char_traits<char>, std::allocator<char> > >*)+0x43) [0x55dee4f01753]
2019-04-17T23:51:44.684 INFO:tasks.ceph.mon.a.smithi002.stderr: 7: (Elector::start()+0x2c2) [0x55dee4fa23a2]
```

06/06/2021 2/4
#2 - 04/22/2019 05:52 PM - Sage Weil
- Status changed from 12 to Fix Under Review

https://github.com/ceph/ceph/pull/27707

(looks like the buffer is only 100 chars, and /proc/cpuinfo frequently exceeds that)

#3 - 04/22/2019 05:52 PM - Sage Weil
- Backport set to nautilus, mimic, luminous

https://github.com/ceph/ceph/pull/27707

(looks like the buffer is only 100 chars, and /proc/cpuinfo frequently exceeds that)

#4 - 04/22/2019 11:32 PM - Brad Hubbard
- Status changed from Fix Under Review to In Progress

#5 - 04/23/2019 06:05 PM - Sage Weil
- Status changed from In Progress to Pending Backport

#6 - 04/25/2019 07:46 AM - Nathan Cutler
- Copied to Backport #39474: luminous: segv in fgets() in collect_sys_info reading /proc/cpuinfo added

#7 - 04/25/2019 07:46 AM - Nathan Cutler
- Copied to Backport #39475: mimic: segv in fgets() in collect_sys_info reading /proc/cpuinfo added

#8 - 04/25/2019 07:46 AM - Nathan Cutler
- Copied to Backport #39476: nautilus: segv in fgets() in collect_sys_info reading /proc/cpuinfo added

#9 - 12/19/2019 02:21 PM - Nathan Cutler
- Pull request ID set to 27707
While running with --resolve-parent, the script "backport-create-issue" noticed that all backports of this issue are in status "Resolved" or "Rejected".