Alpine Linux - Bug #5487

open-vm-tools segfaults on alpine 3.3.3

04/25/2016 05:14 AM - Danil Eremeev

Status:	Closed	**Start date:**	04/25/2016
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	3.5.1		
Affected versions:	3.3.3	**Security IDs:**	

Description

alpine 64bit version

```
#uname -a
Linux 4.1.20-0-grsec #1-Alpine SMP Mon Mar 21 15:49:51 GMT 2016 x86_64 Linux
```

dmesg show

```
<6>[412712.171407] vmtoolsd[32665]: segfault at 0 ip 00006aad80d079a1 sp 0000701c0a273070 error 4
in libvmtools.so.0.0.0[6aad80cd4000+282000]
<1>[412712.171434] grsec: From 192.168.112.159: Segmentation fault occurred at           (nil) in
 /usr/bin/vmtoolsd[vmtoolsd:32665] uid/euid:1001/1001 gid/egid:1001/1001, parent /bin/bash[bash:32
653] uid/euid:1001/1001 gid/egid:1001/1001
```

when start vmtoolsd manually i see only

```
Segmentation fault (core dumped)
```

Associated revisions

Revision 8b24ae01 - 01/02/2017 10:58 AM - Natanael Copa

main/open-vm-tools: fix segfault in error reporting

ref #5487

Revision 0261cb84 - 01/02/2017 11:17 AM - Natanael Copa

main/open-vm-tools: fix segfault in error reporting

fixes #5487

Revision dc9c45b8 - 01/04/2017 04:06 PM - Natanael Copa

main/open-vm-tools: fix the strerror_r patch

fixes #5487

History

#1 - 06/07/2016 05:10 PM - John Longe

This happens on 3.4 as well, but only with the linux-virtgrsec kernel. It does not crash with linux-grsec -- which pulls in open-vm-tools-grsec, by the way.

#2 - 08/23/2016 09:48 AM - Oluf Lorenzen

This is still an issue with Linux 4.4.17, non-grsec/vanilla...

#3 - 11/22/2016 11:20 PM - Fahad Yousuf

As of 3.4.6 running kernel 4.4.30-0-grsec, the issue is still present. Relevant information below:

@alpine-server: ~ (root) # dmesg | tail -n 2
[27.766767] vmtoolsd[2938]: segfault at 0 ip 00007869ba355b0e sp 00007c5f049f25e0 error 4 in libvmtools.so.0.0.0[7869ba324000+280000]
[27.766814] grsec: Segmentation fault occurred at (nil) in /usr/bin/vmtoolsd[vmtoolsd:2938] uid/euid:0/0 gid/egid:104/104, parent /bin/busybox[init:1] uid/euid:0/0 gid/egid:0/0

alpine-server: ~ (root) # uname -a
Linux alpine-server 4.4.30-0-grsec #1-Alpine SMP Mon Nov 7 20:19:21 GMT 2016 x86_64 GNU/Linux@

#4 - 11/22/2016 11:23 PM - Fahad Yousuf

As of 3.4.6 running kernel 4.4.30-0-grsec, the issue is still present. Relevant information below:

```
alpine-server: ~ (root) # dmesg | tail -n 2
[ 27.766767] vmtoolsd2938: segfault at 0 ip 00007869ba355b0e sp 00007c5f049f25e0 error 4 in libvmtools.so.0.0.
0[7869ba324000+280000]
[ 27.766814] grsec: Segmentation fault occurred at (nil) in /usr/bin/vmtoolsd[vmtoolsd:2938] uid/euid:0/0 gid/
egid:104/104, parent /bin/busybox[init:1] uid/euid:0/0 gid/egid:0/0

alpine-server: ~ (root) # uname -a
Linux alpine-server 4.4.30-0-grsec #1-Alpine SMP Mon Nov 7 20:19:21 GMT 2016 x86_64 GNU/Linux
```

#5 - 12/26/2016 06:53 PM - Natanael Copa

reported on irc:

```
alpine-linux1:~# /usr/bin/vmtoolsd
Segmentation fault (core dumped)

alpine-linux1:~# tail -5 /var/log/messages
Dec 26 18:15:00 alpine-linux1 cron.info crond[3321]: USER root pid 3841 cmd run-parts /etc/periodic/15min
Dec 26 18:30:00 alpine-linux1 cron.info crond[3321]: USER root pid 3851 cmd run-parts /etc/periodic/15min
Dec 26 18:45:00 alpine-linux1 cron.info crond[3321]: USER root pid 3853 cmd run-parts /etc/periodic/15min
Dec 26 18:50:43 alpine-linux1 kern.info kernel: [73390.348292] vmtoolsd[3856]: segfault at 0 ip 0000713bae5a0b
63 sp 00007fe2ab94b490 error 4 in libvmtools.so.0.0.0[713bae56f000+280000]
Dec 26 18:50:43 alpine-linux1 kern.alert kernel: [73390.348335] grsec: From 10.47.11.10: Segmentation fault oc
curred at            (nil) in /usr/bin/vmtoolsd[vmtoolsd:3856] uid/euid:0/0 gid/egid:0/0, parent /bin/busybox[
ash:3437] uid/euid:0/0 gid/egid:0/0
```

#6 - 12/26/2016 06:55 PM - Natanael Copa

- Target version set to 3.5.1

#7 - 12/27/2016 09:17 PM - Natanael Copa

I tried it on vmware fusion on mac. I can not reproduce it there.

What version of open-vm-tools is it? What does `vmtoolsd --version` say?

#8 - 12/31/2016 05:37 PM - Fahad Yousuf

Here is my setup.

alpine-server: ~ (root) # vmtoolsd --version
VMware Tools daemon, *version 10.0.7.52125 (build-3227872)
*alpine-server: ~ (root) # cat /proc/cpuinfo
processor : 0
vendor_id : GenuineIntel
cpu family : 6
model : 26
model name : Intel(R) Core(TM) i7-2630QM CPU [at] 2.00GHz
stepping : 4
microcode : 0x25
cpu MHz : 1995.467
cache size : 6144 KB
physical id : 0
siblings : 1
core id : 0
cpu cores : 1
apicid : 0
initial apicid : 0
fpu : yes
fpu_exception : yes
cpuid level : 11
wp : yes
flags : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush dts mmx fxsr sse sse2 ss syscall nx rdtscp lm
constant_tsc arch_perfmon pebs bts nopl xtopology tsc_reliable nonstop_tsc aperfmperf pni ssse3 cx16 sse4_1 sse4_2 x2apic popcnt
tsc_deadline_timer hypervisor lahf_lm ida arat epb pln pts dtherm tsc_adjust
bugs :
bogomips : 3992.22

clflush size : 64
cache_alignment : 64
address sizes : 42 bits physical, 48 bits virtual
power management:
alpine-server: ~ (root) # uname -a
Linux alpine-server 4.4.30-0-grsec #1-Alpine SMP Mon Nov 7 20:19:21 GMT 2016 x86_64 GNU/Linux

#9 - 01/02/2017 10:14 AM - Natanael Copa

Got access to a system where it can be reproduced.

Output of strace:

```
socket(AF_VSOCK, SOCK_STREAM, 0)        = 8
open("/dev/vsock", O_RDONLY)            = 9
ioctl(9, IOCTL_VMCI_SOCKETS_GET_LOCAL_CID or IOCTL_VM_SOCKETS_GET_LOCAL_CID, 0x70a3fc42f994) = 0
close(9)                                = 0
bind(8, {sa_family=AF_VSOCK, sa_data="\0\0\377\3\0\0\365@\33q\0\0\0\0"}, 16) = 0
connect(8, {sa_family=AF_VSOCK, sa_data="\0\0\320\3\0\0\0\0\0\0\0\0"}, 16) = -1 ETIMEDOUT (Operation timed
 out)
brk(0x32ec73ab000)                      = 0x32ec73ab000
--- SIGSEGV {si_signo=SIGSEGV, si_code=SEGV_MAPERR, si_addr=NULL} ---
+++ killed by SIGSEGV (core dumped) +++
Segmentation fault
```

Backtrace:

```
#0  0x000079a440aa0b63 in Err_Errno2String () from /usr/lib/libvmtools.so.0
(gdb) bt
#0  0x000079a440aa0b63 in Err_Errno2String () from /usr/lib/libvmtools.so.0
#1  0x000079a440aae3c5 in Socket_ConnectVMCI () from /usr/lib/libvmtools.so.0
#2  0x000079a440aaddb4 in ?? () from /usr/lib/libvmtools.so.0
#3  0x000079a440aad613 in RpcChannel_Start () from /usr/lib/libvmtools.so.0
#4  0x000079a440aad87d in RpcChannel_Send () from /usr/lib/libvmtools.so.0
#5  0x0000045343f52791 in ?? ()
#6  0x000079a440aad1c5 in RpcChannel_Dispatch () from /usr/lib/libvmtools.so.0
#7  0x000079a440aaec14 in ?? () from /usr/lib/libvmtools.so.0
#8  0x000079a440aaf196 in ?? () from /usr/lib/libvmtools.so.0
#9  0x000079a440379b96 in g_main_context_dispatch ()
   from /usr/lib/libglib-2.0.so.0
#10 0x000079a440379e16 in ?? () from /usr/lib/libglib-2.0.so.0
#11 0x000079a44037a0da in g_main_loop_run () from /usr/lib/libglib-2.0.so.0
#12 0x0000045343f50208 in ?? ()
#13 0x0000045343f4f678 in main ()
```

So what happens, the connect to /dev/vsock times out and vmtoolsd segfaults when trying to generate a string with the errno string.

#10 - 01/02/2017 10:26 AM - Natanael Copa

I know whats wrong. They assume GNU variant of strerror_r:

https://github.com/vmware/open-vm-tools/blob/master/open-vm-tools/lib/err/errPosix.c#L67

```
#if defined(linux) && !defined(N_PLAT_NLM) && !defined(__ANDROID__)
   p = strerror_r(errorNumber, buf, bufSize);
#else
   p = strerror(errorNumber);
#endif
```

#11 - 01/02/2017 11:22 AM - Natanael Copa

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset 0261cb8455c87b5167be9eb0129a177b0578189e.

#12 - 01/04/2017 04:01 PM - Natanael Copa

- Status changed from Resolved to New

the patch is broken. reopening.

#13 - 01/04/2017 04:07 PM - Natanael Copa

- Status changed from New to Resolved

Applied in changeset dc9c45b8ff236147bd2c27482f42ca783a8d5d10.

#14 - 01/24/2017 10:26 AM - Natanael Copa

- Status changed from Resolved to Closed