Subject: oops in khelper
Posted by vaverin on Fri, 09 Nov 2007 11:17:38 GMT
View Forum Message <> Reply to Message

Hello Steve,

Could you please take a look at the following oops? It looks like it is related
to cifs:
1) Code line is corrupted (21 byte?!?), It looks like part of CIFS smb_hdr with
 CIFS magic:
 00 00 50 ff 53 4d 42 32 00 00 00 00 80 41 c0 <00> 00 00 00 00 00
         FF S M B

2) This issue was reproduced several times on several nodes, but every time it
was occurred after the following message:

"CIFS VFS: Invalid size SMB length 4 pdu_length 4"

Is it probably known issue for you?

Thank you,
 Vasily Averin

Virtuozzo/OpenVZ linux kernel Team

Unable to handle kernel NULL pointer dereference at virtual address 00000611
 printing eip:
02106330
*pde = 00004001
Oops: 0002 [#1]
SMP
Modules linked in: nls_iso8859_1 cifs simfs mptctl vzrst vzcpt ip_vzredir
vzredir vzcompat vzdquota vzfs vzethdev vzevent vzlist vzstat ip_vznetstat
af_packet 8021q bridge vznet vznetstat vzmon vzdev iptable_filter tun ipt_mac
ipt_MASQUERADE ip_nat_irc ip_nat_ftp iptable_nat ip_conntrack_irc
ip_conntrack_ftp ipt_LOG ipt_state ip_conntrack ipt_length ipt_ttl ipt_tcpmss
ipt_TCPMSS iptable_mangle ipt_multiport ipt_limit ipt_tos ipt_REJECT ip_tables
thermal processor fan button battery ac uhci_hcd ehci_hcd e752x_edac edac_mc
e1000 sg
CPU: 2, VCPU: 0:1
EIP: 0060:[<02106330>]   Tainted: P   VLI
EFLAGS: 00010202   (2.6.9-023stab044.4-enterprise)
EIP is at kernel_thread+0x0/0xd0
eax: 00000611   ebx: ca969e68   ecx: ca969e28   edx: 00000206
esi: 08109000   edi: ca969e2c   ebp: 00000206   esp: 0814bf30
ds: 007b   es: 007b   ss: 0068
Process khelper (pid: 14, veid=0, threadinfo=0814a000 task=08147360)
Stack: 0213f828 0213f750 ca969e68 00000611 ca969e68 0213fe33 ca969e68 0814bf74

00000000 08109028 08109010 08109018 0213f800 ca969e28 0814a000 ffffffff
ffffffff 00000001 00000000 02123680 00010000 00000000 e1f718c0 ffffffff
Call Trace:
[<0213f828>] __call_usermodehelper+0x28/0x70
[<0213f750>] wait_for_helper+0x0/0xb0
[<0213fe33>] worker_thread+0x1f3/0x280
[<0213f800>] __call_usermodehelper+0x0/0x70
[<02123680>] default_wake_function+0x0/0x20
[<02123680>] default_wake_function+0x0/0x20
[<0213fc40>] worker_thread+0x0/0x280
[<02144d6d>] kthread+0xbd/0x100
[<02144cb0>] kthread+0x0/0x100
[<02106321>] kernel_thread_helper+0x5/0x14
Code: 24 ec 64 50 02 89 44 24 04 e8 1d 64 02 00 83 c4 18 5b 5e 5f c3 89 f6 89 d0
52 ff d3 00 00 50 ff 53 4d 42 32 00 00 00 00 80 41 c0 <00> 00 00 00 00 e5 6c
02 8b 54 24 68 85 c0 75 19 b8 00 e0 ff

Oct 20 03:51:05 kernel: CIFS VFS: Invalid size SMB length 4 pdu_length 4
Oct 20 03:51:05 kernel: CIFS VFS: No response for cmd 50 mid 17053
Oct 20 03:52:37 kernel: Unable to handle kernel NULL pointer dereference at
virtual address 00000611

Oct 26 00:50:22 s39 kernel: CIFS VFS: Invalid size SMB length 4 pdu_length 4
Oct 26 00:50:22 s39 kernel: CIFS VFS: No response for cmd 50 mid 32013
Oct 26 00:50:40 s39 kernel: Unable to handle kernel NULL pointer dereference at
virtual address 00000611

Nov 5 03:50:18 s39 kernel: CIFS VFS: Invalid size SMB length 4 pdu_length 4
Nov 5 03:50:18 s39 kernel: CIFS VFS: No response for cmd 50 mid 10169
Nov 5 03:50:39 s39 kernel: Unable to handle kernel NULL pointer dereference at
virtual address 00000611

Subject: Re: [linux-cifs-client] oops in khelper
Posted by Jeff Layton on Fri, 09 Nov 2007 12:04:32 GMT
View Forum Message <> Reply to Message

On Fri, 09 Nov 2007 14:17:38 +0300
Vasily Averin <vvs@sw.ru> wrote:

> Hello Steve,
>
> Could you please take a look at the following oops? It looks like it
> is related to cifs:
> 1) Code line is corrupted (21 byte?!?), It looks like part of CIFS
> smb_hdr with CIFS magic:
> 00 00 50 ff 53 4d 42 32 00 00 00 00 80 41 c0 <00> 00 00 00 00 00

> FF S M B
>
> 2) This issue was reproduced several times on several nodes, but
> every time it was occurred after the following message:
>
> "CIFS VFS: Invalid size SMB length 4 pdu_length 4"
>
> Is it probably known issue for you?
>
> Thank you,
> Vasily Averin
>
> Virtuozzo/OpenVZ linux kernel Team
>
> Unable to handle kernel NULL pointer dereference at virtual address
> 00000611 printing eip:
> 02106330
> *pde = 00004001
> Oops: 0002 [#1]
> SMP
> Modules linked in: nls_iso8859_1 cifs simfs mptctl vzrst vzcpt
> ip_vzredir vzredir vzcompat vzdquota vzfs vzethdev vzevent vzlist
> vzstat ip_vznetstat af_packet 8021q bridge vznet vznetstat vzmon
> vzdev iptable_filter tun ipt_mac ipt_MASQUERADE ip_nat_irc ip_nat_ftp
> iptable_nat ip_conntrack_irc ip_conntrack_ftp ipt_LOG ipt_state
> ip_conntrack ipt_length ipt_ttl ipt_tcpmss ipt_TCPMSS iptable_mangle
> ipt_multiport ipt_limit ipt_tos ipt_REJECT ip_tables thermal
> processor fan button battery ac uhci_hcd ehci_hcd e752x_edac edac_mc
> e1000 sg CPU: 2, VCPU: 0:1
> EIP: 0060:[<02106330>]   Tainted: P   VLI
> EFLAGS: 00010202   (2.6.9-023stab044.4-enterprise)
> EIP is at kernel_thread+0x0/0xd0
> eax: 00000611   ebx: ca969e68   ecx: ca969e28   edx: 00000206
> esi: 08109000   edi: ca969e2c   ebp: 00000206   esp: 0814bf30
> ds: 007b   es: 007b   ss: 0068
> Process khelper (pid: 14, veid=0, threadinfo=0814a000 task=08147360)
> Stack: 0213f828 0213f750 ca969e68 00000611 ca969e68 0213fe33 ca969e68
> 0814bf74 00000000 08109028 08109010 08109018 0213f800 ca969e28
> 0814a000 ffffffff ffffffff 00000001 00000000 02123680 00010000
> 00000000 e1f718c0 ffffffff Call Trace:
> [<0213f828>] __call_usermodehelper+0x28/0x70
> [<0213f750>] wait_for_helper+0x0/0xb0
> [<0213fe33>] worker_thread+0x1f3/0x280
> [<0213f800>] __call_usermodehelper+0x0/0x70
> [<02123680>] default_wake_function+0x0/0x20
> [<02123680>] default_wake_function+0x0/0x20
> [<0213fc40>] worker_thread+0x0/0x280
> [<02144d6d>] kthread+0xbd/0x100

> [<02144cb0>] kthread+0x0/0x100
> [<02106321>] kernel_thread_helper+0x5/0x14
> Code: 24 ec 64 50 02 89 44 24 04 e8 1d 64 02 00 83 c4 18 5b 5e 5f c3
> 89 f6 89 d0 52 ff d3 00 00 50 ff 53 4d 42 32 00 00 00 00 80 41 c0
> <00> 00 00 00 00 00 e5 6c 02 8b 54 24 68 85 c0 75 19 b8 00 e0 ff
>
>
> Oct 20 03:51:05 kernel: CIFS VFS: Invalid size SMB length 4
> pdu_length 4 Oct 20 03:51:05 kernel: CIFS VFS: No response for cmd
> 50 mid 17053 Oct 20 03:52:37 kernel: Unable to handle kernel NULL
> pointer dereference at virtual address 00000611
>
> Oct 26 00:50:22 s39 kernel: CIFS VFS: Invalid size SMB length 4
> pdu_length 4 Oct 26 00:50:22 s39 kernel: CIFS VFS: No response for
> cmd 50 mid 32013 Oct 26 00:50:40 s39 kernel: Unable to handle kernel
> NULL pointer dereference at virtual address 00000611
>
> Nov 5 03:50:18 s39 kernel: CIFS VFS: Invalid size SMB length 4
> pdu_length 4 Nov 5 03:50:18 s39 kernel: CIFS VFS: No response for
> cmd 50 mid 10169 Nov 5 03:50:39 s39 kernel: Unable to handle kernel
> NULL pointer dereference at virtual address 00000611
> _____
> linux-cifs-client mailing list
> linux-cifs-client@lists.samba.org
> https://lists.samba.org/mailman/listinfo/linux-cifs-client
>

Looks like the random memory corruption I was chasing around a month
ago. It's a nasty bug. This patch from the cifs-2.6 git tree will
probably fix it:

commit c18c732ec6bf372aa959ca6534cbfc32e464defd
Author: Steve French <sfrench@us.ibm.com>
Date: Wed Oct 17 18:01:11 2007 +0000

    [CIFS] fix bad handling of EAGAIN error on kernel_recvmsg in cifs_demultiplex_thread

--
Jeff Layton <jlayton@redhat.com>