
Subject: NFSv3 client OOPS during LTP test
Posted by [den](#) on Tue, 15 May 2007 10:52:20 GMT
[View Forum Message](#) <> [Reply to Message](#)

Hello, All!

I have run LTP over NFSv3 with O_DIRECT support with the default mount options:

```
artemis ~/src/linux-2.6.21.1 $ cat /proc/mounts | fgrep nfs
192.168.1.9:/home/den/tmp /mnt nfs
rw,vers=3,rsiz=131072,wsiz=131072,hard,proto=tcp,timeo=600
,retrans=2,sec=sys,addr=192.168.1.9
0 0
artemis ~/src/linux-2.6.21.1 $
```

The result is an OOPS during "diotest4" testcase, which is 100% triggered in less than 30 seconds:

```
Unable to handle kernel NULL pointer dereference at 0000000000000000 RIP:
[<ffffffff8047e944>] tcp_sendpage+0x370/0x620
PGD 13c6dc067 PUD 13c7ef067 PMD 0
Oops: 0000 [1] SMP
CPU 1
Modules linked in: xt_length ipt_ttl xt_tcpmss iptable_mangle
iptables_filter xt_multiport xt_limit ipt_tos ipt_REJECT ip_tables x_tables
Pid: 4556, comm: diotest4 Not tainted 2.6.21.1 #2
RIP: 0010:[<ffffffff8047e944>] [<ffffffff8047e944>]
tcp_sendpage+0x370/0x620
RSP: 0018:ffff81013c551b98 EFLAGS: 00010246
RAX: 0000000000000000 RBX: 0000000000001000 RCX: 0000000000000000
RDX: 0000000000000000 RSI: 0000000000007d30 RDI: 00000000000005a8
RBP: ffff81013c70f900 R08: 0000000000004040 R09: ffffffff8051cee0
R10: 0000000000000000 R11: 0000000000000000 R12: ffff81013c0e2c80
R13: 0000000000000001 R14: 0000000000004040 R15: 0000000000000000
FS: 00002b9d5b3efb00(0000) GS:ffff81013fc78d40(0000) knlGS:0000000000000000
CS: 0010 DS: 0000 ES: 0000 CR0: 000000008005003b
CR2: 0000000000000000 CR3: 000000013d467000 CR4: 000000000000006e0
Process diotest4 (pid: 4556, threadinfo ffff81013c550000, task
ffff81013fe7ade0)
Stack: ffff810100001000 ffffffff804d9719 000000003c13c000 0000000000000000
0000000000000000 000005a800007c70 0000000000001000 0000000000000000
0000000000000000 0000000000000000 0000000000000000 0000000000001000
Call Trace:
[<ffffffff804d9719>] xs_send_kvec+0x8c/0x95
[<ffffffff804d9856>] xs_sendpages+0x134/0x1d8
[<ffffffff804d9ab2>] xs_tcp_send_request+0x5b/0x123
[<ffffffff804d8bce>] xprt_transmit+0xc1/0x1a2
```

```
[<ffffff802def2d>] nfs3_xdr_writeargs+0x0/0x84
[<ffffff804d744c>] call_transmit+0x1f7/0x231
[<ffffff804dbf0a>] __rpc_execute+0x7e/0x223
[<ffffff802e2464>] nfs_file_direct_write+0x4b5/0x5b8
[<ffffff8026c003>] do_sync_write+0xc8/0x10b
[<ffffff8034036e>] write_chan+0x30f/0x32d
[<ffffff802223ae>] __wake_up+0x36/0x4c
[<ffffff80239384>] autoremove_wake_function+0x0/0x2e
[<ffffff8033adb7>] tty_ldisc_deref+0x5f/0x71
[<ffffff8033b3eb>] tty_write+0x217/0x22c
[<ffffff8026c0f5>] vfs_write+0xaf/0x131
[<ffffff8026c22a>] sys_write+0x45/0x6e
[<ffffff802092ee>] system_call+0x7e/0x83
```

Code: 8b 02 f6 c4 40 74 04 48 8b 52 10 f0 ff 42 08 49 63 c5 48 8b

```
[root@artemis den]# uname -a
Linux artemis.sw.ru 2.6.21.1 #2 SMP Tue May 15 14:42:39 MSD 2007 x86_64
x86_64 x86_64 GNU/Linux
[root@artemis den]#
```

Regards,
Den
