
Subject: [PATCH v2] SUNRPC: skip dead but not buried clients on PipeFS events
Posted by [Stanislav Kinsbursky](#) on Fri, 20 Apr 2012 14:11:02 GMT

[View Forum Message](#) <> [Reply to Message](#)

v2: atomic_inc_return() was replaced by atomic_inc_not_zero().

These clients can't be safely dereferenced if their counter is 0.

Signed-off-by: Stanislav Kinsbursky <skinsbursky@parallels.com>

net/sunrpc/clnt.c | 3 ++-

1 files changed, 2 insertions(+), 1 deletions(-)

diff --git a/net/sunrpc/clnt.c b/net/sunrpc/clnt.c

index 6797246..d10ebc4 100644

--- a/net/sunrpc/clnt.c

+++ b/net/sunrpc/clnt.c

```
@@ -218,7 +218,8 @@ static struct rpc_clnt *rpc_get_client_for_event(struct net *net, int event)
     if (((event == RPC_PIPEFS_MOUNT) && clnt->cl_dentry) ||
         ((event == RPC_PIPEFS_UMOUNT) && !clnt->cl_dentry))
         continue;
-    atomic_inc(&clnt->cl_count);
+    if (atomic_inc_not_zero(&clnt->cl_count) == 0)
+        continue;
     spin_unlock(&sn->rpc_client_lock);
     return clnt;
 }
```
