
Subject: [PATCH] SUNRPC: register PipeFS file system after pernet sybsystem
Posted by [Stanislav Kinsbursky](#) on Thu, 05 Apr 2012 17:04:37 GMT

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

PipeFS superblock creation routine relays on SUNRPC pernet data presense, which is created on register_pernet_subsys() call in SUNRPC module init function. Registering of PipeFS filesystem prior to registering of per-net subsystem leads to races (mount of PipeFS can dereference uninitialized data).

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

net/sunrpc/sunrpc_syms.c | 17 ++++++-----
1 files changed, 9 insertions(+), 8 deletions(-)

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

index 8adfc88..3d6498a 100644

--- a/net/sunrpc/sunrpc_syms.c

+++ b/net/sunrpc/sunrpc_syms.c

@@ -75,20 +75,21 @@ static struct pernet_operations sunrpc_net_ops = {

static int __init

init_sunrpc(void)

{

- int err = register_rpc_pipefs();

+ int err = rpc_init_mempool();

if (err)

goto out;

- err = rpc_init_mempool();

- if (err)

- goto out2;

err = rpcauth_init_module();

if (err)

- goto out3;

+ goto out2;

cache_initialize();

err = register_pernet_subsys(&sunrpc_net_ops);

if (err)

+ goto out3;

+

+ err = register_rpc_pipefs();

+ if (err)

goto out4;

#ifdef RPC_DEBUG

rpc_register_sysctl();

@@ -98,11 +99,11 @@ init_sunrpc(void)

return 0;

```
out4:
- rpcauth_remove_module();
+ unregister_pernet_subsys(&sunrpc_net_ops);
out3:
- rpc_destroy_mempool();
+ rpcauth_remove_module();
out2:
- unregister_rpc_pipefs();
+ rpc_destroy_mempool();
out:
    return err;
}
```
