Subject: [PATCH 2.6.25] [ATM] Oops reading net/atm/arp
Posted by den on Thu, 10 Jan 2008 11:25:47 GMT
View Forum Message <> Reply to Message

cat /proc/net/atm/arp causes the NULL pointer dereference in the
get_proc_net+0xc/0x3a. This happens as proc_get_net believes that the
parent proc dir entry contains struct net.

Fix this assumption for "net/atm" case.

The problem is introduced by the commit c0097b07abf5f92ab135d024dd41bd2aada1512f
from Eric W. Biederman/Daniel Lezcano.

Signed-off-by: Denis V. Lunev <den@openvz.org>

```
diff --git a/fs/proc/proc_net.c b/fs/proc/proc_net.c
index cfc4f6c..4823c96 100644
--- a/fs/proc/proc_net.c
+++ b/fs/proc/proc_net.c
@@ -96,6 +96,17 @@ static struct proc_dir_entry *proc_net_shadow(struct task_struct *task,
  return task->nsproxy->net_ns->proc_net;
 }

+struct proc_dir_entry *proc_net_mkdir(struct net *net, const char *name,
+  struct proc_dir_entry *parent)
+{
+ struct proc_dir_entry *pde;
+ pde = proc_mkdir_mode(name, S_IRUGO | S_IXUGO, parent);
+ if (pde != NULL)
+  pde->data = net;
+ return pde;
+}
+EXPORT_SYMBOL_GPL(proc_net_mkdir);
+
 static __net_init int proc_net_ns_init(struct net *net)
 {
  struct proc_dir_entry *root, *netd, *net_statd;
@@ -107,18 +118,16 @@ static __net_init int proc_net_ns_init(struct net *net)
   goto out;

  err = -EEXIST;
- netd = proc_mkdir("net", root);
+ netd = proc_net_mkdir(net, "net", root);
  if (!netd)
   goto free_root;
```

```
  err = -EEXIST;
- net_statd = proc_mkdir("stat", netd);
+ net_statd = proc_net_mkdir(net, "stat", netd);
  if (!net_statd)
   goto free_net;

  root->data = net;
- netd->data = net;
- net_statd->data = net;

  net->proc_net_root = root;
  net->proc_net = netd;
diff --git a/include/linux/proc_fs.h b/include/linux/proc_fs.h
index a531682..8f92546 100644
--- a/include/linux/proc_fs.h
+++ b/include/linux/proc_fs.h
@@ -201,6 +201,8 @@ static inline struct proc_dir_entry *create_proc_info_entry(const char
*name,
 extern struct proc_dir_entry *proc_net_fops_create(struct net *net,
  const char *name, mode_t mode, const struct file_operations *fops);
 extern void proc_net_remove(struct net *net, const char *name);
+extern struct proc_dir_entry *proc_net_mkdir(struct net *net, const char *name,
+ struct proc_dir_entry *parent);

 #else

diff --git a/net/atm/proc.c b/net/atm/proc.c
index 5d9d5ff..565e75e 100644
--- a/net/atm/proc.c
+++ b/net/atm/proc.c
@@ -476,7 +476,7 @@ static void atm_proc_dirs_remove(void)
   if (e->dirent)
    remove_proc_entry(e->name, atm_proc_root);
  }
- remove_proc_entry("atm", init_net.proc_net);
+ proc_net_remove(&init_net, "atm");
 }

 int __init atm_proc_init(void)
@@ -484,7 +484,7 @@ int __init atm_proc_init(void)
  static struct atm_proc_entry *e;
  int ret;

- atm_proc_root = proc_mkdir("atm", init_net.proc_net);
+ atm_proc_root = proc_net_mkdir(&init_net, "atm", init_net.proc_net);
  if (!atm_proc_root)
   goto err_out;
  for (e = atm_proc_ents; e->name; e++) {
```

Subject: Re: [PATCH 2.6.25] [ATM] Oops reading net/atm/arp
Posted by davem on Thu, 10 Jan 2008 11:51:51 GMT
View Forum Message <> Reply to Message

From: "Denis V. Lunev" <den@openvz.org>
Date: Thu, 10 Jan 2008 14:28:53 +0300

> cat /proc/net/atm/arp causes the NULL pointer dereference in the
> get_proc_net+0xc/0x3a. This happens as proc_get_net believes that the
> parent proc dir entry contains struct net.
>
> Fix this assumption for "net/atm" case.
>
> The problem is introduced by the commit c0097b07abf5f92ab135d024dd41bd2aada1512f
> from Eric W. Biederman/Daniel Lezcano.
>
> Signed-off-by: Denis V. Lunev <den@openvz.org>

Applied, thanks.