Subject: [PATCH net-2.6.26][IPV6]: Fix potential net leak and oops in ipv6 routing code.
Posted by Pavel Emelianov on Wed, 26 Mar 2008 15:55:47 GMT
View Forum Message <> Reply to Message

The commits f3db4851 ([NETNS][IPV6] ip6_fib - fib6_clean_all handle several network namespaces) and 69ddb805 ([NETNS][IPV6] route6 - Make proc entry /proc/net/rt6_stats per namespace) made some proc files per net.

Both of them introduced potential OOPS - get_proc_net can return NULL, but this check is lost - and a struct net leak - in case single_open() fails the previously got net is not put.

Kill all these bugs with one patch.

Signed-off-by: Pavel Emelyanov <xemul@openvz.org>

```
diff --git a/net/ipv6/route.c b/net/ipv6/route.c
index ac44283..cd82b6d 100644
--- a/net/ipv6/route.c
+++ b/net/ipv6/route.c
@@ -2390,10 +2390,18 @@ static int ipv6_route_show(struct seq_file *m, void *v)

 static int ipv6_route_open(struct inode *inode, struct file *file)
 {
+ int err;
  struct net *net = get_proc_net(inode);
  if (!net)
   return -ENXIO;
- return single_open(file, ipv6_route_show, net);
+
+ err = single_open(file, ipv6_route_show, net);
+ if (err < 0) {
+  put_net(net);
+  return err;
+ }
+
+ return 0;
 }

 static int ipv6_route_release(struct inode *inode, struct file *file)
@@ -2429,8 +2437,18 @@ static int rt6_stats_seq_show(struct seq_file *seq, void *v)

 static int rt6_stats_seq_open(struct inode *inode, struct file *file)
 {
+ int err;
```

```
  struct net *net = get_proc_net(inode);
- return single_open(file, rt6_stats_seq_show, net);
+ if (!net)
+  return -ENXIO;
+
+ err = single_open(file, rt6_stats_seq_show, net);
+ if (err < 0) {
+  put_net(net);
+  return err;
+ }
+
+ return 0;
 }

 static int rt6_stats_seq_release(struct inode *inode, struct file *file)
```

Subject: Re: [PATCH net-2.6.26][IPV6]: Fix potential net leak and oops in ipv6 routing code.
Posted by Daniel Lezcano on Wed, 26 Mar 2008 15:59:29 GMT
View Forum Message <> Reply to Message

Pavel Emelyanov wrote:
> The commits f3db4851 ([NETNS][IPV6] ip6_fib - fib6_clean_all handle several
> network namespaces) and 69ddb805 ([NETNS][IPV6] route6 - Make proc entry
> /proc/net/rt6_stats per namespace) made some proc files per net.
>
> Both of them introduced potential OOPS - get_proc_net can return NULL, but
> this check is lost - and a struct net leak - in case single_open() fails the
> previously got net is not put.
>
> Kill all these bugs with one patch.
>
> Signed-off-by: Pavel Emelyanov <xemul@openvz.org>
>
> ---
>
> diff --git a/net/ipv6/route.c b/net/ipv6/route.c
> index ac44283..cd82b6d 100644
> --- a/net/ipv6/route.c
> +++ b/net/ipv6/route.c
> @@ -2390,10 +2390,18 @@ static int ipv6_route_show(struct seq_file *m, void *v)
>
> static int ipv6_route_open(struct inode *inode, struct file *file)
> {
> + int err;
>   struct net *net = get_proc_net(inode);
>   if (!net)

```
>    return -ENXIO;
> - return single_open(file, ipv6_route_show, net);
> +
> + err = single_open(file, ipv6_route_show, net);
> + if (err < 0) {
> +  put_net(net);
> +  return err;
> + }
> +
> + return 0;
>  }
>
>  static int ipv6_route_release(struct inode *inode, struct file *file)
> @@ -2429,8 +2437,18 @@ static int rt6_stats_seq_show(struct seq_file *seq, void *v)
>
>  static int rt6_stats_seq_open(struct inode *inode, struct file *file)
>  {
> + int err;
>   struct net *net = get_proc_net(inode);
> - return single_open(file, rt6_stats_seq_show, net);
> + if (!net)
> +  return -ENXIO;
> +
> + err = single_open(file, rt6_stats_seq_show, net);
> + if (err < 0) {
> +  put_net(net);
> +  return err;
> + }
> +
> + return 0;
>  }
>
>  static int rt6_stats_seq_release(struct inode *inode, struct file *file)
```

Good catch. Thanks.

Acked-by: Daniel Lezcano <dlezcano@fr.ibm.com>

Subject: Re: [PATCH net-2.6.26][IPV6]: Fix potential net leak and oops in ipv6 routing code.

Posted by davem on Wed, 26 Mar 2008 23:50:02 GMT

View Forum Message <> Reply to Message

From: Daniel Lezcano <dlezcano@fr.ibm.com>
Date: Wed, 26 Mar 2008 16:59:29 +0100

> Pavel Emelyanov wrote:

> > The commits f3db4851 ([NETNS][IPV6] ip6_fib - fib6_clean_all handle several
> > network namespaces) and 69ddb805 ([NETNS][IPV6] route6 - Make proc entry
> > /proc/net/rt6_stats per namespace) made some proc files per net.
> >
> > Both of them introduced potential OOPS - get_proc_net can return NULL, but
> > this check is lost - and a struct net leak - in case single_open() fails the
> > previously got net is not put.
> >
> > Kill all these bugs with one patch.
> >
> > Signed-off-by: Pavel Emelyanov <xemul@openvz.org>
 ...
> Good catch. Thanks.
>
> Acked-by: Daniel Lezcano <dlezcano@fr.ibm.com>

Applied, thanks everyone!
