
Subject: Re: [PATCH] iptables compat code error way & module refcounting fix
Posted by [Patrick McHardy](#) on Mon, 30 Oct 2006 15:45:19 GMT

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

Dmitry Mishin wrote:

> This patch fixes bug in iptables modules refcounting on compat error way.

>

> As we are getting modules in check_compat_entry_size_and_hooks(), in case of
> later error, we should put them all in translate_compat_table(), not in the
> compat_copy_entry_from_user() or compat_copy_match_from_user(), as it is now.

>

> Signed-off-by: Dmitry Mishin <dim@openvz.org>

> Acked-by: Vasily Averin <vvv@openvz.org>

> Acked-by: Kirill Korotaev <dev@openvz.org>

>

> ip_tables.c | 36 ++++++-----

> 1 file changed, 11 insertions(+), 25 deletions(-)

>

> ----

> @@ -1618,7 +1603,7 @@ translate_compat_table(const char *name,

> unsigned int *hook_entries,

> unsigned int *underflows)

> {

> - unsigned int i;

> + unsigned int i, j;

> struct xt_table_info *newinfo, *info;

> void *pos, *entry0, *entry1;

> unsigned int size;

> @@ -1636,21 +1621,21 @@ translate_compat_table(const char *name,

> }

>

> duprintf("translate_compat_table: size %u\n", info->size);

> - i = 0;

> + j = 0;

> xt_compat_lock(AF_INET);

> /* Walk through entries, checking offsets. */

> ret = IPT_ENTRY_ITERATE(entry0, total_size,

> check_compat_entry_size_and_hooks,

> info, &size, entry0,

> entry0 + total_size,

> - hook_entries, underflows, &i, name);

> + hook_entries, underflows, &j, name);

> if (ret != 0)

> goto out_unlock;

>

> ret = -EINVAL;

> - if (i != number) {

> + if (j != number) {

```
> duprintf("translate_compat_table: %u not %u entries\n",
> - i, number);
> + j, number);
> goto out_unlock;
> }
>
> @@ -1709,6 +1694,7 @@ translate_compat_table(const char *name,
> free_newinfo:
> xt_free_table_info(newinfo);
> out:
> + IPT_ENTRY_ITERATE(entry0, total_size, cleanup_entry, &j);
> return ret;
> out_unlock:
> xt_compat_unlock(AF_INET);
>
```

This doesn't look right, if we fail at `xt_alloc_table_info` for example the module references are not released. What case exactly is this patch supposed to fix?
