Subject: Re: Kernel OOPS with kernel 2.6.18 and openvz 0.28.18.1
Posted by MrDigi on Mon, 14 May 2007 22:21:47 GMT
View Forum Message <> Reply to Message

That oops occurs in:

net/ipv6/netfilter/ip6_tables.c:

```
void ip6t_unregister_table(struct xt_table *table)
{
	struct xt_table_info *private;
	void *loc_cpu_entry;
	struct module *me;

	me = table->me; <--- HERE is OOPSed, so table was null
	...
```

It was called from:
net/ipv6/netfilter/ip6table_mangle.c

```
void fini_ip6table_mangle(void)
{
	nf_unregister_hooks(ip6t_ops, ARRAY_SIZE(ip6t_ops));
	ip6t_unregister_table(ve_packet_mangler);
#ifdef CONFIG_VE_IPTABLES
	ve_packet_mangler = NULL;
#endif
}
```

I think the problem is somewhere here in cleanup:

net/ipv6/netfilter/ip6table_mangle.c

```
int init_ip6table_mangle(void)
{
	int ret;
	struct ip6t_table *tmp_mangler;

	/* Register table */
	tmp_mangler = ip6t_register_table(&packet_mangler,
			&initial_table.repl);
	if (IS_ERR(tmp_mangler))
		return PTR_ERR(tmp_mangler);
#ifdef CONFIG_VE_IPTABLES
	ve_packet_mangler = tmp_mangler;
#endif
```

```
        /* Register hooks */
        ret = nf_register_hooks(ip6t_ops, ARRAY_SIZE(ip6t_ops));
        if (ret < 0)
                goto cleanup_table;

        return ret;

 cleanup_table:
        ip6t_unregister_table(ve_packet_mangler);
#ifdef CONFIG_VE_IPTABLES
        ve_packet_mangler = NULL;
#endif
        return ret;
}
}
---
```

So perhaps something like the following two added lines are enough ?!

```
---
void ip6t_unregister_table(struct xt_table *table)
{
        struct xt_table_info *private;
        void *loc_cpu_entry;
        struct module *me;

+         if (table == null)
+           return;

        me = table->me; <--- HERE is OOPSed, so table was null
        ...
---
```

Best regards
Thimo