Subject: [NET][IA64] Unaligned access in sk_run_filter
Posted by Mishin Dmitry on Mon, 20 Feb 2006 15:28:28 GMT
View Forum Message <> Reply to Message

Hello,

We have an issue on ia64 box. It is easy triggerable 'kernel unaligned access'
in sk_run_filter:

```
        ptr = load_pointer(skb, k, 4, &tmp);
        if (ptr != NULL) {
                A = ntohl(*(u32 *)ptr); << here
                continue;
        }
```

due to 'k' is coming from userspace it can be easy triggered, e.g.:
[root@node1 ~]# tcpdump -i eth0 'ip[1:2]=0'

Could you advise how to fix this?

--
Thanks,
Dmitry.

Subject: Re: [NET][IA64] Unaligned access in sk_run_filter
Posted by Jes Sorensen on Mon, 20 Feb 2006 15:43:16 GMT
View Forum Message <> Reply to Message

>>>>> "Dmitry" == Dmitry Mishin <dim@openvz.org> writes:

Dmitry> Hello, We have an issue on ia64 box. It is easy triggerable
Dmitry> 'kernel unaligned access' in sk_run_filter:

```
Dmitry>         ptr = load_pointer(skb, k, 4, &tmp);
Dmitry>         if (ptr != NULL) {
Dmitry>                 A = ntohl(*(u32 *)ptr); << here
```

Change the above line to something like this:

```
                A = ntohl(get_unaligned((u32*)ptr));
```

And add an #include <asm/unaligned.h>

Cheers,
Jes