
Subject: Re: [patch 0/1][NETNS49] Make af_unix autobind per namespace
Posted by [Daniel Lezcano](#) on Tue, 02 Oct 2007 20:51:51 GMT
[View Forum Message](#) <> [Reply to Message](#)

Eric W. Biederman wrote:

> Daniel Lezcano <dlezcano@fr.ibm.com> writes:
>
>> The following patch change autobind fonction to use the ordernum
>> from the network namespace instead of using the local static variable.
>
> Why do we care?
> Information leak?
> Some application is expecting a predictable autobind value?
>
> Just skimming the code it looks like it will work correctly without
> this.

I think my summary is ... too short :)

I don't see any applications taking care of this. If they ask for an abstract socket, then they don't care about the bind result. So probably, the patchset is totally useless.

But from the POV of the checkpoint/restart, we should check if this value is somewhere visible from userspace and so storable by an application.

It appears this is the case with /proc/net/unix, where an abstract socket is symbolized by the path pattern "@". Example:

```
cat /proc/net/unix
```

```
Num      RefCount Protocol Flags   Type St Inode Path
c6a27710: 00000002 00000000 00000000 0002 01  4357 @00003
```

I agree by the fact that can be considered as a detail and the probability to have an application storing this informaton is very small (eg. checkpointing while doing netstat in the container). But IMHO, the paradigm "never seen from userspace" fails and that justifies to have the ordernum variable relative to a namespace.

-- Daniel

Containers mailing list
Containers@lists.linux-foundation.org
<https://lists.linux-foundation.org/mailman/listinfo/containers>
