Subject: Re: nscd on VE
Posted by maratrus on Sat, 02 Feb 2008 13:25:19 GMT
View Forum Message <> Reply to Message

Hi,

I'm very sorry for delay.

As we can see from strace output setuid and setgid capabilities are not sufficient. We need also CAP_AUDIT_WRITE.

From src/include/linux/capability.h (openvz kernel tree) inside VE we should to set SETVEID capability and "man vzctl" allows us to do this. I tried this but suddenly found that this capability was not actually set. The reason is in kernel's do_env_create() function which is called when we start our VPS. It displaces setveid capability otherwise this VPS becomes the serious hole in security.

So I can suggest you two ways:
1. If it is possible you can use the elder version of nscd. I noticed that it doesn't try to set this capabilities. (I experimented with VPS based on Fedora 4).
2. You can compile nscd by yourself. We easily can find the relevant piece of code and can try to comment unnecessary string.