

---

Subject: OpenVZ precreated template root compromised ?  
Posted by [akbardotinfo](#) on Sun, 16 Jun 2013 15:49:55 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

Dear All,

we're using centos-6.x86\_64-devel with cpanel software installed.  
the cpanel staff said that my server is root compromised.

But after I redownload the precreated template of openvz, it's same as is. the  
/lib64/libkeyutils.so.1.3.0\* is on all precreated template of openvz (it exist on precreated centos-5  
(/lib64/libkeyutils.so.1.2) also on openvz.org/Download/template/precreated

Below is the cpanel staff said:

Hello,

It appears that your server has been compromised with a malicious payload designed to sniff for  
and steal server passwords. Everything that we know about this payload and identifying it can be  
found here:

[go.cpanel.net/checkyourserver](http://go.cpanel.net/checkyourserver)

We've essentially used these same steps on that page to confirm that your server has been  
compromised such as the following:

```
[root@4246999~]cPs# ls -lah /lib*/libkeyutils*  
lrwxrwxrwx 1 root root 20 Apr 24 06:06 /lib64/libkeyutils.so.1 -> libkeyutils.so.1.3.0*  
-rwxr-xr-x 1 root root 10K Jun 22 2012 /lib64/libkeyutils.so.1.3*  
-rwxr-xr-x 1 root root 32K Jun 22 2012 /lib64/libkeyutils.so.1.3.0*
```

```
[root@4246999~]cPs# rpm -qf /lib64/libkeyutils.so.1.3.0  
file /lib64/libkeyutils.so.1.3.0 is not owned by any package
```

Any suggestion ?

---