Subject: Dangerous updates?
Posted by rollinw on Tue, 03 Oct 2006 16:47:26 GMT
View Forum Message <> Reply to Message

Our system is based on CentOS 4.3 using the latest released test vzkernel. We run Suse 9.3 x8_64 as our VPSs.

Recently a developer not experienced in OpenVZ attempted to run SUSE System Updates from YaST on a VPS. YaST, very obligingly, tried to install all the system updates, including those for the SUSE kernel. What happened was not pretty. Apparently parts of the vzkernel were modified, and CentOS libraries were updated. After YaST was run on all the VPSs, once they were stopped, they would no longer start correctly. Init would die while trying to initialize the programs in /etc/init.d/, and only a skeleton system would start up. One could enter the VPS and start init level 3 things manually, but they would no longer get started by the system.

Well, we tried destroying the bad VPSs and re-creating them. This did not change the startup problem. We tried uninstalling the VZkernel OS rpm, and then re-installing it. This also did not solve the problem. We ended up re-installing CentOS 4.3 and starting from scratch. After that everything worked OK.

The bottom line here is a question. Is the use of yast (or yum) inside a VPS a potential security issue for an entire OpenVZ installation? Has anyone else experience this kind of thing?

I would appreciate your comments on this.

Thanks,
rollinw
Rollin Weeks

Subject: Re: Dangerous updates?
Posted by dlzinc on Mon, 09 Oct 2006 04:57:51 GMT
View Forum Message <> Reply to Message

I use yum all the time on all my VPSes with no problem. OpenVZ's supposed to isolate all the files of each VE from each other so I don't think there's any security problems with it. I've completely destroyed VPSes before (ever tried an in-place replacement of CentOS with Debian + debootstrap?) and a simple nuke and recreate of the VPS would always fix things.

It would've been interesting to see what files outside the VPS were changed, if any...

Subject: Re: Dangerous updates?
Posted by rollinw on Mon, 09 Oct 2006 21:09:56 GMT
View Forum Message <> Reply to Message

If you use Debian for your VHS environments, you may know that Suse has a package system

similar to aptget called YaST. YaST provides ways of updating the entire system, including hardware, software install/remove, and system update. If you run the YaST system update on a Suse-based VHS, YaST attempts to update ALL system packages, including the kernel, with the latest Suse versions. Now a Suse VHS does not know its kernel is really a vzkernel running on CentOS, and it tries to update these files too! That's where the problem is.

Note that yum on the CentOS hardware node works find and, to my knowledge does not create any problems.

Subject: Re: Dangerous updates?
Posted by John Kelly on Thu, 12 Oct 2006 04:48:15 GMT
View Forum Message <> Reply to Message

rollinw wrote on Tue, 03 October 2006 12:47Is the use of yast (or yum) inside a VPS a potential security issue for an entire OpenVZ installation? Has anyone else experience this kind of thing?

I have a suse 9.3 VE running on a debian HN. I use yast online update in the VE. It does not update any kernel, because I do not have a kernel installed in the VE. But even if there was a kernel installed in the VE, it would not matter. From inside the VE, you can't alter any HN files or libraries, because they are outside the chrooted VE.

Maybe something else caused the problems you described, and the guilty party is not aware of their error.

Subject: Re: Dangerous updates?
Posted by rollinw on Thu, 12 Oct 2006 20:09:46 GMT
View Forum Message <> Reply to Message

John,

What you say makes sense, because a VPS has no /boot for a kernel file to reside in and no kernel components under /usr. Still, I saw what happened to us, and I am a bit uneasy about upgrades or patches to parts of /lib or /lib64 or /usr/lib or /etc.

For a Suse 9.3 VPS I discovered that Yast2 keeps very good records (logs) of what it does (including a list of all RPMs applied) in /var/log/. Unfortunately, we destroyed all this trail of information when we got rid of the bad VPSs.

I am considering setting up another host that already has a VZ OS installed and attempting to duplicate the behavior we had with yast previously. It depends on whether our people consider it a high priority.

rollinw

Rollin Weeks

Subject: Re: Dangerous updates?
Posted by rollinw on Mon, 23 Oct 2006 16:10:29 GMT
View Forum Message <> Reply to Message

After spending quite a bit of time on this problem, I have managed to reproduce part of the problem. I have created a VPS that will not start up properly. In this case, the HN did not seem to be affected. Here is the sequence that has led to the defective VPSs:

1. Inside the SUSE VPS bring up the Yast (ncurses) inteface.
   (This is a SuSE 9.3 SMP x86_64 kernel).
2. Find a mirror that has updates (RPM patches).
3. Run the online update application.
4. After yast compiles its list of updates, select those to be
   installed. We chose 2 categories: recommended and security
5. Yast gives a warning that there is a kernel patch and asks if
   this should be skipped. We chose to install.
6. During the installation of updates, Yast gives an error
   regarding the kernel update, and at this point we chose the
   Skip option. There were 45 update RPMs installed.
7. Yast appeared to complete the update successfully.
8. The VPS continues to run OK after the update until it is
   stopped by vzctl.
9. From this point on, the VPS does not start properly. Vzctl
   start does not give an error message, but only a skeletion
   system comes up. It appears that the boot process does not
   complete correctly. In particular, init 3 does not start
   up the processes in /etc/init.d One can enter the VPS and
   start the processes manually, including the system logger,
   the network, sshd, etc.

I have gone through the Yast logs and the /var/log/messages file,
but so far I have only part of the answer. Yast does attempt to
install a version of the Suse kernel. It creates a /boot directory and attempts to write a vmlinux kernel file and an initrd. This is the point at which it fails. But it does install a new kernel RPM, which is older than the version running on the HN.

Besides the kernel install problem, there seems to be a problem resulting from the linux-utils RPM. This is suggested from the time stamp when this was installed. Here are the contents of the messages log that show the failure(s) that occurred:

Oct 13 21:54:07 vpssuse1 usermod[32604]: default group changed - account=nobody, uid=65534, gid=65533, old gid=65533, by=0
Oct 13 21:54:13 vpssuse1 groupadd[32681]: group already exists - group=haldaemon, by=0

Oct 13 21:54:13 vpssuse1 useradd[32682]: account already exists - account=haldaemon, by=0
Oct 13 21:54:16 vpssuse1 init: Trying to re-exec init
Oct 13 21:54:16 vpssuse1 init: no more processes left in this runlevel
Oct 13 21:54:20 vpssuse1 init: Trying to re-exec init
Oct 13 21:54:20 vpssuse1 init: no more processes left in this runlevel
Oct 13 21:54:37 vpssuse1 groupadd[1422]: group already exists - group=sshd, by=0
Oct 13 21:54:37 vpssuse1 useradd[1423]: account already exists - account=sshd, by=0
Oct 13 22:00:01 vpssuse1 run-crons[1607]: mcelog returned 1
Oct 13 22:01:47 vpssuse1 syslog-ng[19545]: new configuration initialized

---

I am trying to understand how vzctl starts a VPS. I examined quite a bit of the code and discovered that some time after vzctl mounts the VPS, it calls a routine, execvp() that at some point calls the /sbin/init inside the VPS. I have not been able to discover the other steps in the VPS startup.

Repeating my earlier comment, this update does not appear to have damaged the HN, because I can still create new VPSs and start them correctly.

Rollin