Subject: vzkernel-3.10.0-x releases stopped since Sept?
Posted by websavers on Fri, 30 Nov 2018 19:22:23 GMT
View Forum Message <> Reply to Message

Hey OpenVZ devs... where are the security patched kernels for OpenVZ 7?

We get regular email alerts about security patches to both OpenVZ 6 and 7, yet only the OpenVZ 6 kernels have been released in the repos since September, despite multiple patches having been developed for the OpenVZ 7 kernel.

It's one thing to block the open source community's access to the ReadyKernel patches (even though many of us would surely pay for a KernelCare-like licensing structure for this feature), but a whole other, much more serious, thing to not even release security-patched kernel versions...

What's going on here?

And while we're on the topic, shouldn't these OpenVZ 7 kernel updates that never actually get compiled and released to the repos be set up with an RSS feed on openvz.org like the OpenVZ 6 kernel updates are?

Subject: Re: vzkernel-3.10.0-x releases stopped since Sept?
Posted by khorenko on Mon, 03 Dec 2018 15:03:30 GMT
View Forum Message <> Reply to Message

Answered to the part about rare stable kernel updates at
https://bugs.openvz.org/browse/OVZ-7070

websavers wrote on Fri, 30 November 2018 22:22And while we're on the topic, shouldn't these OpenVZ 7 kernel updates that never actually get compiled and released to the repos be set up with an RSS feed on openvz.org like the OpenVZ 6 kernel updates are?

Those tags are compiled and put into factory repo (nightly)
https://download.openvz.org/virtuozzo/factory/x86_64/os/Packages/v/
but they are not fully tested - there could be several builds a day, surely they don't pass full QA cycle - thus they are not marked stable and not put to stable repo.

Subject: Re: vzkernel-3.10.0-x releases stopped since Sept?
Posted by websavers on Mon, 03 Dec 2018 15:13:35 GMT
View Forum Message <> Reply to Message

So you're essentially saying:

1. The Virtuozzo devs only care about the security of OpenVZ 6 because you're stuck patching it still, and
2. The Virtuozzo devs think it's acceptable to leave their kernel vulnerable on countless OpenVZ 7

systems because the people that are using it should be paying you for a full Virtuozzo license if they want security.

That's pretty absurd. If I were running KVM on a CentOS 7 box, I would receive kernel patches as they are released by the CentOS 7 development team. At bare minimum Virtuozzo 7 should get a similar kernel patch/release cycle as CentOS 7 to apply the upstream kernel patches, even if that doesn't include OpenVZ 7 specific patches.

All that this policy does is serve to push people away from OpenVZ 7 to alternate platforms that don't treat security so poorly, which means your team's possibility of upgrading OpenVZ 7 users to a full Virtuozzo 7 license gets even slimmer. Why would you want to encourage that?

Subject: Re: vzkernel-3.10.0-x releases stopped since Sept?
Posted by khorenko on Mon, 03 Dec 2018 16:10:54 GMT
View Forum Message <> Reply to Message

i'm essentially saying that Virtuozzo devs work on Virtuozzo - payed version - and do as much as they can to make OpenVZ users happy, but with no additional devs/QA efforts (which are unpayed, sorry).
And building stable kernels + readykernel patches - are efforts, it cannot be automated.
And TESTING them are BIG efforts, because tests do fail and QA (humans!) have to investigate issues.

Quote:2. The Virtuozzo devs think it's acceptable to leave their kernel vulnerable on countless OpenVZ 7 systems because the people that are using it should be paying you for a full Virtuozzo license if they want security.
Surely not. i personally just think that people who use OpenVZ (and want to save their money) are quite experienced (otherwise how do they run business without support?).
And if so, they can build kernels with security fixes themselves. This is a payment for saving money.

And again - this is my personal opinion only,
and people who make business decisions might have different ones.

Subject: Re: vzkernel-3.10.0-x releases stopped since Sept?
Posted by TomB on Mon, 03 Dec 2018 19:58:01 GMT
View Forum Message <> Reply to Message

There are also community users who use this technology for different projects..

Virtuozzo only gets positive name recognition by tackling this and publishing stable releases, including security updates. The use of OpenVZ and therefore also Virtuozzo will only decrease, while the product is good and powerful!
Compare it with the competitors. OpenVZ integration/support has been removed from many products.

I think that more priority should be given to OVZ7. Still the best solution for containers and I do not intend to use LXC or Proxmox :blush:

Subject: Re: vzkernel-3.10.0-x releases stopped since Sept?
Posted by devnull on Wed, 05 Dec 2018 22:55:37 GMT

View Forum Message <> Reply to Message

Hello. :)

Please forgive my bad English, I am French...

Quote:And if so, they can build kernels with security fixes themselves. This is a payment for saving money.

Seems legit! (and fair IMHO)

Just one question, is there somewhere a guide (even a short note would be fine) to build a kernel - marked as stable - plus security fixes?

Have a nice day!

Subject: Re: vzkernel-3.10.0-x releases stopped since Sept?
Posted by devnull on Sat, 15 Dec 2018 22:07:53 GMT

View Forum Message <> Reply to Message

Hello. :)

Sorry for the late answer.

In short: compiling the latest* OpenVZ 7 kernel, released on Github, was a breeze and everything seems alright!

* => rh7-3.10.0-862.20.2.vz7.73.9 (Nov 24, 2018)

But I am just curious: are GitHub releases "flagged" as stable or not?

I mean, should I use src.openvz.org instead?

Many thanks for your answers.

Subject: Re: vzkernel-3.10.0-x releases stopped since Sept?
Posted by TomB on Mon, 17 Dec 2018 07:51:47 GMT

View Forum Message <> Reply to Message

devnull wrote on Sat, 15 December 2018 23:07Hello. :)

Sorry for the late answer.

In short: compiling the latest* OpenVZ 7 kernel, released on Github, was a breeze and everything seems alright!

* => rh7-3.10.0-862.20.2.vz7.73.9 (Nov 24, 2018)

But I am just curious: are GitHub releases "flagged" as stable or not?

I mean, should I use src.openvz.org instead?

Many thanks for your answers.

You can also use the factory kernel.

Quote:Those tags are compiled and put into factory repo (nightly)
https://download.openvz.org/virtuozzo/factory/x86_64/os/Pack ages/v/

We need a test-method to report kernel-bugs.

Subject: Re: vzkernel-3.10.0-x releases stopped since Sept?
Posted by khorenko on Wed, 19 Dec 2018 09:59:09 GMT
View Forum Message <> Reply to Message

Sorry for the late answer.

devnull wrote on Sun, 16 December 2018 01:07But I am just curious: are GitHub releases "flagged" as stable or not?

I mean, should I use src.openvz.org instead?

Nope, they are not marked, and there no flags on src.openvz.org as well,
but you can get a list of stable kernels checking the yum repo:

http://repo.virtuozzo.com/vz/releases/
http://download.openvz.org/virtuozzo/releases/

Subject: Re: vzkernel-3.10.0-x releases stopped since Sept?
Posted by khorenko on Wed, 19 Dec 2018 10:23:50 GMT
View Forum Message <> Reply to Message

devnull wrote on Thu, 06 December 2018 01:55Just one question, is there somewhere a guide (even a short note would be fine) to build a kernel - marked as stable - plus security fixes?

i'd say the easiest way is to

* get src.rpm of the latest stable kernel,
* unpack it "# rpm -ihv vzkernel-...src.rpm",
* get patches you want to apply (for example take from the devel email list or from vzkernel git tree)
  You can also take a look at the list of issues listed at ReadyKernel site - just for the reference which are worth to apply.
* put additional patches to apply into ~/rpmbuild/SOURCES/ and edit ~/rpmbuild/SPEC/kernel.spec to apply new patches
  (take a look how it's done for linux-kernel-test.patch kernel.spec, do it similarly)
* don't forget to add some suffix to "%define ovzver" in kernel.spec
* and finally compile the kernel, command example:

```
# cd ~/rpmbuild/SOURCES/ && rpmbuild -v --define "_sourcedir $PWD" -ba ../SPEC/kernel.spec
```

Or you can

* clone vzkernel git tree
* checkout latest stable by tag
* apply new patches you want (may be just cherry-pick them from later branches)

* prepare a cumulative patch using a command for example:

```
# git diff rh7-3.10.0-862.14.4.el7 | filterdiff -p 1 --clean -x configs/\* -x config.OpenVZ\* | xz > ~/rpmbuild/SOURCES/patch-ovz.xz
```

(instead of "rh7-3.10.0-862.14.4.el7" you should use a tags for RHEL kernel which your stable kernel is based on)
For example for vzkernel-3.10.0-862.11.6.vz7.64.7.x86_64.rpm the RHEL tag is "rh7-3.10.0-862.11.6.vz7.64.7.el7"

* don't forget to add some suffix to "%define ovzver" in kernel.spec
* and finally compile the kernel, command example:

```
# cd ~/rpmbuild/SOURCES/ && rpmbuild -v --define "_sourcedir $PWD" -ba ../SPEC/kernel.spec
```

Subject: Re: vzkernel-3.10.0-x releases stopped since Sept?
Posted by devnull on Thu, 20 Dec 2018 23:25:18 GMT

View Forum Message <> Reply to Message

@khorenko: many thanks for your detailed reply and for your time! :)

Because I am not familiar with Git (cherry-pick) and CentOS specific syntax, I will need some time to learn and test.

I will answer in this topic as soon as I manage to build a "custom" vzkernel + security patches.

Have a great day!

Subject: Re: vzkernel-3.10.0-x releases stopped since Sept?
Posted by TomB on Wed, 26 Dec 2018 10:44:58 GMT
View Forum Message <> Reply to Message

Unfortunately. I have found an alternative solution for public hosting of my projects.

Kernel patching does indeed take a lot of time and I can understand it. I can't guarantee the stability and reliability without these patches.
I am grateful that you all are still investing time in OVZ7. It is still the most powerful free-to-use solution for containers.

Thanks!

Subject: Re: vzkernel-3.10.0-x releases stopped since Sept?
Posted by websavers on Fri, 28 Dec 2018 02:30:23 GMT
View Forum Message <> Reply to Message

khorenko wrote on Mon, 03 December 2018 12:10i'm essentially saying that Virtuozzo devs work on Virtuozzo - payed version - and do as much as they can to make OpenVZ users happy, but with no additional devs/QA efforts (which are unpayed, sorry).
And building stable kernels + readykernel patches - are efforts, it cannot be automated.
And TESTING them are BIG efforts, because tests do fail and QA (humans!) have to investigate issues.

I do actually completely understand that you'd want to invest as little time as possible into maintaining the open source base systems. This is why I suggested keeping these types of releases strictly to security patches released to the upstream CentOS kernel, and nothing more.

My suggestion is that *after* these patches have been tested as readykernel patches (which the dev team has to do anyway for commercial customers), the same patches/diffs be applied to the currently stable kernel release, compiled, then quickly tested to confirm the kernel boots successfully, then released to the repo (or perhaps the testing repo for a week before being moved to release).

To further save time investment, every time a ReadyKernel patch is created, the same diffs could be quickly applied to the stable kernel on a test box. Then once a month, a cron script could freshly compile and install the testing kernel and reboot the box. Upon successful reboot it would upload the new kernel release to the repo. If the automated compiling and reboot fails, then it seems plausible the failure could be helpful feedback for devs and likely for ReadyKernel commercial customers as well.

A couple notes on this:

- Doing this should be considerably more stable for end-users than suggesting that they use factory kernel versions. And it would be much more secure for end-users than not getting security patches for 60+ days as it will result in a security patched kernel release roughly once a month. End-users can then choose whether they want to reboot into it immediately or a bit later to keep their reboots to a minimum.
- Ultimately, devs already have to do the work of testing the exact same patches via ReadyKernel, so this work does not need to be duplicated or wasted time. The only additional dev time would be the act of applying the patches to the current release kernel. Even the act of installing the kernel on a test box and rebooting the box to ensure it comes back online could be automated as described above. A seasoned kernel dev would take probably 15 minutes to do this with automation and 60 minutes without automation each month.

Yes, this means a small amount of additional dev time monthly, but it also means you're sending important messages:

1. When users of OpenVZ 6 need to make the decision to choose either OpenVZ 7 or move to a different virtualisation system (which is going to happen en masse in the next year due to OpenVZ6 EOL Nov 2019), that the OpenVZ 7 transition is the simplest and optimal way forward because it does not present them with new security challenges, as compared to vz6.
2. That Virtuozzo Linux 7 is at least on par security-wise with CentOS 7, which nobody can say is the case at the moment since security patches for Virtuozzo 7 are often delayed by months as compared to CentOS 7.

I've heard that Virtuozzo is preparing for stand-alone release of ReadyKernel and regardless of whether the Virtuozzo devs decide to do any of the above, I'll be first in line to purchase and use ReadyKernel on our OpenVZ 7 nodes. I do, however, still hope that you'll do something like what's described above to ensure that those who do not opt for a ReadyKernel subscription can best maintain the security of their nodes.

While I don't think this is nearly as comprehensive a solution, I'm grateful that @khorenko provided the rough steps to download the kernel sources, apply security patches, and compile the patched kernel. If that could be expanded into a more comprehensive wiki entry, I think that would be a great, albeit somewhat less useful, alternative.

Subject: Re: vzkernel-3.10.0-x releases stopped since Sept?
Posted by wishd on Sat, 26 Jan 2019 19:18:58 GMT

View Forum Message <> Reply to Message

As far as I am aware (Correct me if I am wrong khorenko)

There should be 4 stable kernel releases a year. This means for security, you'll need to create your kernels from the patches. Excellent info above to do so, thanks. Or use factory kernel in a pinch. Someone could take this, and spin off a more secure version - I know Solar Designer in the mailing list seem to be going that way.

For the 4 releases a year, I don't know if there is a road map on when they would be released. That info would be good to have.

Its unfortunate ready kernel can not be purchased as an addon and the paid openvz support that used to be available is gone - but that is the way it is. Your choice is to build yourself, or look to lxc/lxd or kvm as an alternative.

A bit unrelated kinda funny that Acronis releases their software like acronis gateway using "virtuozzo linux" and also has the very old kernels on their latest software.

Subject: Re: vzkernel-3.10.0-x releases stopped since Sept?
Posted by wishd on Tue, 12 Feb 2019 16:51:11 GMT
View Forum Message <> Reply to Message

The team has released a new kernel:
https://lists.openvz.org/pipermail/users/2019-February/00755 5.html

To address CVE-2019-5736

Thank you Konstantin Khorenko and Virtuozzo team.

Subject: Re: vzkernel-3.10.0-x releases stopped since Sept?
Posted by khorenko on Tue, 12 Feb 2019 19:51:02 GMT
View Forum Message <> Reply to Message

:) :roll: