Subject: Spectre and Meltdown Patch ASAP Please
Posted by vztester on Thu, 04 Jan 2018 09:04:18 GMT
View Forum Message <> Reply to Message

RHEL already has a patch out and this may be the most important patch for OpenVZ.
On that note it sounds like it would be impacted, can any OpenVZ devs comment if they know for sure Spectre and Meltdown apply here?

AFAIK I would expect and assume so and this is a so-called doomsday scenario if an attacker can gain access to other containers' or hostnode memory.

Subject: Re: Spectre and Meltdown Patch ASAP Please
Posted by suhailc on Thu, 04 Jan 2018 15:17:08 GMT
View Forum Message <> Reply to Message

Please confirm when an OpenVZ kernel patch will be out.

RHEL and CentOS kernel patches are already out.

Subject: Re: Spectre and Meltdown Patch ASAP Please
Posted by vztester on Thu, 04 Jan 2018 19:36:08 GMT
View Forum Message <> Reply to Message

Just bumping this hoping for some news and ETA ASAP.

Thanks OpenVZ team we appreciate the project, know you are busy and normally I am more patient but this is urgent.

Subject: Re: Spectre and Meltdown Patch ASAP Please
Posted by bjdea1 on Fri, 05 Jan 2018 00:39:17 GMT
View Forum Message <> Reply to Message

Yes please let us know when an OpenVZ patch comes out. Waiting patiently.

Subject: Re: Spectre and Meltdown Patch ASAP Please
Posted by vzbuccaneer on Fri, 05 Jan 2018 02:26:16 GMT
View Forum Message <> Reply to Message

While it is understandable that considerable effort may be required to adapt and test security updates released by RHEL for the OpenVZ kernel. What isn't being addressed is the lack of communication since disclosure of the vulnerabilities. The official assessments and White Papers have gone as far to call out OpenVZ directly by name. The severity of these vulnerabilities may vary widely among different virtualization systems, but shared kernel platforms are greatly impacted. Given the severity and the direct mention during disclosure, this issue really warrants a timely response.

RHEL security updates were released on the evening of January 3rd, only a few hours after disclosure. Is there at least a status on a pending kernel update for OpenVZ?

Subject: Re: Spectre and Meltdown Patch ASAP Please
Posted by bomart on Fri, 05 Jan 2018 09:22:25 GMT
View Forum Message <> Reply to Message

The worst part is that there is no official information about the patch.
However, all sources give OpenVZ as vulnerable

Subject: Re: Spectre and Meltdown Patch ASAP Please
Posted by ccto on Fri, 05 Jan 2018 12:46:15 GMT
View Forum Message <> Reply to Message

https://virtuozzo.com/virtuozzo-addresses-intel-bug-question s/

Subject: Re: Spectre and Meltdown Patch ASAP Please
Posted by snajpa on Fri, 05 Jan 2018 15:21:23 GMT
View Forum Message <> Reply to Message

I don't trust OpenVZ team to do anything anymore.

I've ported the 696-18.7 RHEL6 patch over to OpenVZ 042stab126.2

If you don't trust my quick merge repo over here:

https://github.com/snajpa/openvz6-kernel

SRPM here:

http://repo.vpsfree.cz/testing/vzkernel/vzkernel-2.6.32-042s tab126.666.src.rpm

How to install:

Setup up our vpsFree repo: http://repo.vpsfree.cz/testing/vpsfree.repo

yum install vzkernel-2.6.32-042stab126.666

If Red Hat releases more patches, I'll be sure to port them as well.

Stay safe, stay patched. And please migrate off of dead solutions lead by non-transparent almost non-existent team.

Subject: Re: Spectre and Meltdown Patch ASAP Please
Posted by samiam123 on Fri, 05 Jan 2018 17:16:14 GMT
View Forum Message <> Reply to Message

As far as I know there are no known exploits in the wild. So no need to panic just yet. Also, the KernelCare people still have not released a patch and they are usually on top of things. So it must be a complicated one that will take some time. OVZ has been pretty good at security updates so I am sure they will be coming out with a patched kernel soon enough.

That link someone posted further up indicates they are already testing a patched kernel. The fact it has not made it to OVZ kernel yet is not necessarily a bad thing. That means we will probably eventually get a more well tested kernel. There will probably be more kernel updates as changes are better tested. There is also a microcode update from Intel coming so that will be more testing and maybe another patch once that is out. So it's not a quick fix update the kernel and you are done thing.

https://www.cloudlinux.com/cloudlinux-os-blog/entry/intel-cp u-bug-kernelcare-and-cloudlinux

---

Subject: Re: Spectre and Meltdown Patch ASAP Please
Posted by caw0KecCu on Fri, 05 Jan 2018 22:50:11 GMT
View Forum Message <> Reply to Message

There are no OpenVZ team exists anymore, only the Virtuozzo teams exists. Do not expect any free product and service from a for profit company, even if its based on open source and free software (linux kernel). You cannot use OpenVZ7 like you used the OpenVZ6 before (supported only as Virtuozzo with horrible EULA - make sure you check the 2.6 audit rights part).

http://repo.virtuozzo.com/vzlinux/7.4/EULA

Subject: Re: Spectre and Meltdown Patch ASAP Please
Posted by snajpa on Sat, 06 Jan 2018 01:44:17 GMT
View Forum Message <> Reply to Message

If they didn't act as assholes in the bugzilla a long time ago (and that hasn't changed for the better), I would still be happily paying customer for support of an opensource product (had OpenVZ maintenance program for 2 years).

But you can't seriously expect me accepting any EULA, I have no nice words to describe what I'm feeling now.

EULAs belong to the world of M$, not here. Say what you want about for-profit company. Isn't Red Hat now > $2B company? Do they have any other EULA than GPL?

Subject: Re: Spectre and Meltdown Patch ASAP Please
Posted by vaverin on Sat, 06 Jan 2018 11:46:06 GMT
View Forum Message <> Reply to Message

We have released 042stab127.2 kernel

https://openvz.org/Download/kernel/rhel6/042stab127.2

Thank you,
Vasily Averin

Subject: Re: Spectre and Meltdown Patch ASAP Please
Posted by suhailc on Sat, 06 Jan 2018 12:07:35 GMT
View Forum Message <> Reply to Message

Fantastic guys. Let's get patching!

Subject: Re: Spectre and Meltdown Patch ASAP Please
Posted by notbuu on Sat, 06 Jan 2018 12:53:36 GMT
View Forum Message <> Reply to Message

Thank you! Perfect!

Subject: Re: Spectre and Meltdown Patch ASAP Please
Posted by snajpa on Sun, 07 Jan 2018 03:45:12 GMT
View Forum Message <> Reply to Message

```
diff -ruN ./arch/x86/mm/pgtable.c ../linux-16-to-vz/arch/x86/mm/pgtable.c
--- ./arch/x86/mm/pgtable.c     2018-01-07 04:22:45.057056298 +0100
+++ ../linux-16-to-vz/arch/x86/mm/pgtable.c     2018-01-05 08:13:54.251837657 +0100
@@ -325,8 +325,8 @@
        pgd_mop_up_pmds(mm, pgd);
        pgd_dtor(pgd);
        paravirt_pgd_free(mm, pgd);
-       free_pages((unsigned long)pgd, PGD_ALLOCATION_ORDER);
```

```
        mm->nr_ptds--;
+       free_pages((unsigned long)pgd, PGD_ALLOCATION_ORDER);
 }

 int ptep_set_access_flags(struct vm_area_struct *vma,
```

Well, that ^ is the difference between OpenVZ team's patch and mine, otherwise I'm at the same code now, to the last whitespace. I was too lazy here to reorder the lines to make more sense, I knew about this one while I made it.

Hm... OK, next time I surely won't spend the day waiting for OpenVZ team and I will rather get to the porting of RHEL 6 changes right away.

Subject: Re: Spectre and Meltdown Patch ASAP Please
Posted by vaverin on Sun, 07 Jan 2018 08:16:46 GMT
View Forum Message <> Reply to Message

Dear Pavel,

thank you very much for review of our patch.
You're great man if you was able to backport such huge patches correctly.

However I would note that main part of time during release takes not backport of patches, but its careful testing.
In past we have released test kernels, however nobody used it until it was released in stable branch.

Our users hates node reboots, and usually they prefer to wait until someone will check the new kernel.

Thank you,
Vasily Averin

Subject: Re: Spectre and Meltdown Patch ASAP Please
Posted by snajpa on Sun, 07 Jan 2018 13:58:04 GMT
View Forum Message <> Reply to Message

Actually you did most of the work for me. All that was needed is to take Red Hat's 696-16.1 kernel, 696-18.7 kernel and your 126.2 SRPM, patch from there; have two repos, merge 18.7 into 16.7 and vz 042stab126 patch into another 16.7, then merge those two repos - created about 8 merge conflicts easy to resolve, one of them that one I showed you (which ended up being the only difference).

Also Red Hat seems to have forgotten about XSAVEOPT CPUID feature.

So there was nothing to test really, since KAISER didn't touch OpenVZ in any sensitive way.

That is the reason why I'm so curious whey VZ team has lessen it's standards on patch release speed.

You guys used to come before Red Hat, back when Kir and xemul were at their peak productivity) I miss that. A lot!

Subject: Re: Spectre and Meltdown Patch ASAP Please
Posted by HugoRay on Sun, 07 Jan 2018 13:59:46 GMT
View Forum Message <> Reply to Message

That's what I'm bothered with the most too. I'm sure they're working on it, but the lack of communication is bothering me. Why are they so silent about this?

Subject: Re: Spectre and Meltdown Patch ASAP Please
Posted by curx on Sun, 07 Jan 2018 16:26:44 GMT
View Forum Message <> Reply to Message

Hi,

please take a lool at the Announce:

OpenVZ project released an updated RHEL6 based kernel.
Read below for more information. Everyone is advised to update.

Changes and Download
==========
(since 042stab126.2)

* Rebase to RHEL6u9 kernel 2.6.32-696.18.7.el6
* [Important] CVE-2017-5715 triggers the speculative execution by utilizing branch target injection. It relies on the presence of a precisely-defined instruction sequence in the privileged code as well as the fact that memory accesses may cause allocation into the microprocessor's data cache even for speculatively executed instructions that never actually commit (retire). As a result, an unprivileged attacker could use this flaw to cross the syscall and guest/host boundaries and read privileged memory by conducting targeted cache side-channel attacks. (CVE-2017-5715)
* [Important] CVE-2017-5753 triggers the speculative execution by performing a bounds-check bypass. It relies on the presence of a precisely-defined instruction sequence in the privileged code as well as the fact that memory accesses may cause allocation into the microprocessor's data cache even for speculatively executed instructions that never actually commit (retire). As a result, an unprivileged attacker could use this flaw to cross the syscall boundary and read privileged memory by conducting targeted cache side-channel attacks. (CVE-2017-5753)

* [Important] CVE-2017-5754 relies on the fact that, on impacted microprocessors, during speculative execution of instruction permission faults, exception generation triggered by a faulting access is suppressed until the retirement of the whole instruction block. In a combination with the fact that memory accesses may populate the cache even when the block is being dropped and never committed (executed), an unprivileged local attacker could use this flaw to read privileged (kernel space) memory by conducting targeted cache side-channel attacks. (CVE-2017-5754)
* A null-pointer dereference in net/rds/rdma.c:__rds_rdma_map() could allow a local attacker to cause denial of service. (PSBM-79750)
* Start of a container with NFS server inside could result in node crash due to a bug in auth_domain_put(). (PSBM-80028)

For more info and downloads, see:
https://openvz.org/Download/kernel/rhel6/042stab127.2

See also
========
https://access.redhat.com/errata/RHSA-2018:0008
https://www.redhat.com/security/data/cve/CVE-2017-5715.html
https://www.redhat.com/security/data/cve/CVE-2017-5753.html
https://www.redhat.com/security/data/cve/CVE-2017-5754.html

Bug reporting
=============
Use http://bugs.openvz.org/ to report any bugs found.

Regards,
OpenVZ team

Subject: Re: Spectre and Meltdown Patch ASAP Please
Posted by vaverin on Sun, 07 Jan 2018 17:25:03 GMT
View Forum Message <> Reply to Message

Dear Pavel,

we do not 'just repack' stable RHEL kernels, we add own functionality,
we have own original usecases that are out of focus of Red Hat.
We regularly found and report issue affected RHEL and sometime mainline linux kernels.

Last RHEL6 patch was 250+ kB size and changed 180 files,
it was not cosmetic changes that cannot affect our functionality.

We have detected such troubles before.
For example recent stackguard fix broke CPT in vz6 kernel

http://www.openwall.com/lists/oss-security/2017/06/22/6
we timely detected the problem and released fixed kernels
so our users was not noticed it.

This time our testing found that last Red Hat changes broke CRIU,
that's why my collegians have still not released update for Vz/OpenVz 7 (I hope they will finish soon).

The same issue affects vz6 kernels too however our carefull testing did not detected any (new) troubles,
seems criu usecase is really very special.

So please, say thanks to our glorious QA for their hard, important and almost invisible work.

Thank you,
Vasily Averin

Subject: Re: Spectre and Meltdown Patch ASAP Please
Posted by snajpa on Sun, 07 Jan 2018 17:54:51 GMT
View Forum Message <> Reply to Message

Thank you Vasily for your answer!

Now, I know that at times like this, there's too little time to do PR and communicate all of what is going on internally to the outside, but you see...

There's this board, Twitter, IRC, MLs, wiki and I don't know how many other channels, I've monitored most of them, but there was literally no message from you guys in the critical time window for me - I'm sitting on 1700 production containers and have to keep them reasonably up & secure. So when 696-18.7 came out, I became really anxious about not knowing whether I should start porting and testing myself.

I've been running OpenVZ 6 long enough to have approximate knowledge of how it works internally and how it evolved over time, back to 2009, when we started with OpenVZ, which shipped with Debian.

Since then I have even built a start up company based on vz6, which failed to make it commercialy, but we did have vz6 and ZFS integrated the Kubernetes way for our internal deployment back 5 years ago.

I think we share a common vision, how containerization on Linux should be done and how it should be used and deployed.

But I can't agree with the way you're handling it as an open-source project. The world around you guys has moved and now there's a whole bunch of successful open-source based companies, which model you could follow - Jira doesn't quite cut it these days.

I would appreciate to see the QA results live and everything, you're doing basically behind closed doors, to be an open process too. Where money lies in and what I would pay you for, is for ability to have my ticket in a public standard open-source friendly bugzilla (well, or Github...) prioritized. But the way it was with the vz 6 support program...

I think it's not impossible to be fully open, yet commercially successful project - when you let the right people go after selling just what the heck you would do anyway for free. Wouldn't you want to help guys over here while merging and testing the patches together with the community? Could you imagine what we could do if every one of us power vz users had cooperated with you on QA? Shared tests in git repo, deployed in labs all over the planet? I would certainly participate.

But for that, vz7 would have to stay vzkernel+vzctl+libs combo of repositaries, not a complete bundle of heavily modified EL.

I can definitely understand the desire to integrate all to a bundle like that, but that shouldn't come at cost of being able to at least build your stuff from scratch - and create a custom bundle of heavily modified VZ.

vaverin wrote on Sun, 07 January 2018 12:25
[...] that are out of focus of Red Hat.

I definitely know what you're talking about, at 120+ CTs per node and those CTs load variability and their ever increasing size and demand for resources, I can feel the use-cases Red Hat doesn't test.

Or at least didn't with EL6.

But since things are the way they are, we are forced to build our own custom repack of something, with the same goals in mind as you guys.

So we're choosing to do that based on a distro, which is defined declaratively, can be QA-d from scratch on-commit out-of-box; a distro which can be bent so much, we don't have to run along with the inustry's madness with Systemd, LXD, Docker and other bad practice example collections.

So in the end I have much to thank you guys for.

Firstly, for much of the code which is upstream now and which I can now rely and build upon;

secondly, for pioneering containers the right way;

thirdly for CRIU,

and lastly, but this is most important - by publishing your technology as open-source (regardless my reservations here), you've enabled me to pioneer and build
a community-based way of sharing hardware, some would say a community alternative to

commercial hosting; vpsFree.cz (https://vpsfree.org website in English).

It wouldn't exist without OpenVZ, certainly we wouldn't be able to fit so much so comfortably on so little HW, compared to fullvirt-ers.

So there is a lot of things I'm thankful about.

Subject: Re: Spectre and Meltdown Patch ASAP Please
Posted by himbeere on Sun, 07 Jan 2018 19:21:52 GMT
View Forum Message <> Reply to Message

Hello all.

Did you guys experienced any performance dropdowns with to new kernel?

thanks and cheers

Subject: Re: Spectre and Meltdown Patch ASAP Please
Posted by vztester on Sun, 07 Jan 2018 20:41:10 GMT
View Forum Message <> Reply to Message

Thanks OpenVZ team for the patch. I want to say the positive is that we do have an active community and this issue got more people active here in the forums that have been lurking.
It would have been nice for some communication or announcement/timeline, normally I would not be so impatient but in this circumstance it is urgent.

With that said I think we should express more appreciation, OpenVZ is free of charge and has enabled us all to do a lot of amazing things and has been a very rock solid solution that I've used for basically 13 years.

Subject: Re: Spectre and Meltdown Patch ASAP Please
Posted by kapper on Mon, 08 Jan 2018 01:00:34 GMT
View Forum Message <> Reply to Message

Simply thanks for this update and the continued commitment to OpenVZ by the Virtuozzo Company.

Subject: Re: Spectre and Meltdown Patch ASAP Please
Posted by ccto on Mon, 08 Jan 2018 03:43:06 GMT
View Forum Message <> Reply to Message

Me too. - "Simply thanks for this update and the continued commitment to OpenVZ by the Virtuozzo Company."

Especially thank you for the important update in the short period.
(even 3rd party live kernel patch providers stated that it is not easy to import the patch without reboot)

Subject: Re: Spectre and Meltdown Patch ASAP Please
Posted by vaverin on Mon, 08 Jan 2018 08:08:25 GMT
View Forum Message <> Reply to Message

himbeere wrote on Sun, 07 January 2018 22:21Hello all.

Did you guys experienced any performance dropdowns with to new kernel?

thanks and cheers

We did not significant performance dropdown in regular tasks/usecases,
precise performance measurements are planned however are not started yet.

Subject: Re: Spectre and Meltdown Patch ASAP Please
Posted by vaverin on Mon, 08 Jan 2018 17:08:00 GMT
View Forum Message <> Reply to Message

vztester wrote on Sun, 07 January 2018 23:41
It would have been nice for some communication or announcement/timeline, normally I would not be so impatient but in this circumstance it is urgent.

Dear all,

as far as I understan right source of actual information now is Virtuozzo blog
https://virtuozzo.com/blog/
https://virtuozzo.com/virtuozzo-addresses-intel-bug-question s/

Frankly speaking at present it does not look well for me,
however I think we will spend resources to improve it.

Thank you,
Vasily Averin

Subject: Re: Spectre and Meltdown Patch ASAP Please
Posted by vaverin on Tue, 09 Jan 2018 09:24:00 GMT

View Forum Message <> Reply to Message

OpenVZ7 update was released.

It includes new kernel, criu, qemu-kvm and libvirt.

https://download.openvz.org/virtuozzo/releases/openvz-7.0.6- 509/
https://download.openvz.org/virtuozzo/releases/7.0/x86_64/os /repoview/

Thank you,
Vasily Averin

Subject: Re: Spectre and Meltdown Patch ASAP Please
Posted by netio on Fri, 12 Jan 2018 13:09:27 GMT
View Forum Message <> Reply to Message

Hello,

we just experienced a very strange thing. All our centos 6 production servers peaked CPU usage exactly at the same time around 11:45 and at 12:25 it stopped. We found nothing in logs. No crons, no difference in network usage. No evident problematic customer processes. Never happened to us before all those years. Has anyone experienced anything similar? Thanks.

Subject: Re: Spectre and Meltdown Patch ASAP Please
Posted by kapper on Fri, 12 Jan 2018 23:00:38 GMT
View Forum Message <> Reply to Message

I'd remote guess cron-jobs?

Subject: Re: Spectre and Meltdown Patch ASAP Please
Posted by netio on Wed, 17 Jan 2018 10:43:58 GMT
View Forum Message <> Reply to Message

Only standard system crons:
Jan 12 10:01:01 ovz1 run-parts(/etc/cron.hourly)[396825]: finished 0anacron
Jan 12 11:01:01 ovz1 CROND[663113]: (root) CMD (run-parts /etc/cron.hourly)
Jan 12 11:01:01 ovz1 run-parts(/etc/cron.hourly)[663113]: starting 0anacron
Jan 12 11:01:01 ovz1 run-parts(/etc/cron.hourly)[663140]: finished 0anacron
Jan 12 12:01:01 ovz1 CROND[1015674]: (root) CMD (run-parts /etc/cron.hourly)

Subject: Re: Spectre and Meltdown Patch ASAP Please
Posted by bjdea1 on Tue, 23 Jan 2018 23:52:17 GMT

MELTDOWN AND SPECTRE PATCHING HAS BEEN A TOTAL TRAIN WRECK

https://www.wired.com/story/meltdown-spectre-patching-total- train-wreck/

Intel Cans Spectre, Meltdown Patches: What You Need to Know

https://www.tomsguide.com/us/intel-spectre-patch-recall,news -26503.html

Intel Spectre Patches Are "Complete And Utter Garbage" According To Linux Inventor Linus Torvalds

https://segmentnext.com/2018/01/23/intel-spectre-patches-lin ux-inventor/

So does this mean the recent OpenVZ patch is also affected ?