Consider disabling CPU vulnerabilities mitigation features in our Vagrant build box

12/30/2019 07:35 AM - intrigeri

Status: Resolved
Priority: Normal
Assignee:
Category: Build system
Target version: Tails_4.4
Feature Branch: feature/17386-vagrant-disable-cpu-vuln-mitigations
Type of work: Code
Blueprint:

Description
Given the kind of things we do in our Vagrant build box, it seems very unlikely that vulnerabilities such as Spectre and Meltdown can be exploited in there. So perhaps we can reclaim some of the performance cost of the corresponding mitigation features?

This can be done by adding mitigations=off to the kernel command line.

Related issues:
Related to Tails - Feature #17387: Consider disabling CPU vulnerabilities mit... In Progress

Associated revisions
Revision d4722d41 - 12/30/2019 07:56 AM - intrigeri
Vagrant build box: disable mitigation features for CPU vulnerabilities (refs: #17386)

Given the kind of things we do in our Vagrant build box, it seems very unlikely that vulnerabilities such as Spectre and Meltdown can be exploited in there. Let's reclaim some of the performance cost of the corresponding mitigation features.

As of Linux 4.9.189, mitigations=off is equivalent to:

```
nopti nospectre_v1 nospectre_v2 spectre_v2_user=off
spec_store_bypass_disable=off l1tf=off mds=off
```

As of Linux 5.4.5, these extra options are added to the above list:

```
kpti=0 nobp=0 ssbd=force-off tsx_async_abort=off kvm.nx_huge_pages=off
```

Revision b969a33a - 02/29/2020 10:02 PM - segfault
Merge branch 'feature/17386-vagrant-disable-cpu-vuln-mitigations' into stable (Closes: #17386)
Given the kind of things we do in our Vagrant build box, it seems very unlikely that vulnerabilities such as Spectre and Meltdown can be exploited in there. Let's reclaim some of the performance cost of the corresponding mitigation features.

As of Linux 4.9.189, mitigations=off is equivalent to:

```
nopti nospectre_v1 nospectre_v2 spectre_v2_user=off
  spec_store_bypass_disable=off l1tf=off mds=off
```

As of Linux 5.4.5, these extra options are added to the above list:

```
  kpti=0 nobp=0 ssbd=force-off tsx_async_abort=off kvm.nx_huge_pages=off
```

---

**History**

### #1 - 12/30/2019 07:36 AM - intrigeri

Next steps:

- measure if it measurably lowers build time on a developer's system (no nested virt)
- measure if it measurably lowers build time on our CI builders (nested virt)

### #2 - 12/30/2019 07:57 AM - intrigeri

- **Feature Branch set to feature/17386-vagrant-disable-cpu-vuln-mitigations**

### #3 - 12/30/2019 03:57 PM - intrigeri

- **Status changed from In Progress to Needs Validation**
- **Assignee deleted (intrigeri)**
- **Target version set to Tails_4.2**
- **Type of work changed from Test to Code**

- 7% i.e. 2 minutes saved on my laptop (quick SquashFS compression)
- 2% i.e. 30 seconds saved on my local Jenkins (release-time SquashFS compression; also has mitigations=off both in the l0 virtualization host and in the l1 Jenkins slave VM)
- 3.5% i.e. 2.5 minutes saved on lizard (all builders & testers busy; release-time SquashFS compression; has mitigations=auto — the default — both in the l0 virtualization host and in the l1 Jenkins slave VM)

That's not a ton, but it adds up:

- When one is in a dev frenzy and builds lots of images in a day, it starts to make a significant difference.
- Every minute saved on a build job on our CI not only shortens the feedback loop for this build, but in heavy load situations, it also frees the builder VM earlier, which in turn shortens the feedback loop for other, queued jobs.
So IMO we should do it. Thoughts?

#4 - 01/07/2020 06:00 PM - CyrilBrulebois
- Target version changed from Tails_4.2 to Tails_4.3

#5 - 02/03/2020 02:02 PM - hefee
- Assignee set to hefee

#6 - 02/03/2020 02:40 PM - hefee
- Assignee deleted (hefee)

The changes seems fine, but I'm not that deep into the CPU attacks so I don't want to merge it. As I understood correctly this patch is only for the Tails building VM and not for running the test suite?

#7 - 02/03/2020 02:41 PM - hefee
- Status changed from Needs Validation to In Progress
- Assignee set to intrigeri

#8 - 02/03/2020 02:49 PM - intrigeri
- Status changed from In Progress to Needs Validation

As I understood correctly this patch is only for the Tails building VM and not for running the test suite?

Yes.

#9 - 02/03/2020 02:51 PM - intrigeri
- Assignee deleted (intrigeri)

#10 - 02/11/2020 03:26 PM - anonym
- Target version changed from Tails_4.3 to Tails_4.4

#11 - 02/20/2020 06:01 PM - intrigeri
- Related to Feature #17387: Consider disabling CPU vulnerabilities mitigation features in our CI builder/tester VMs added

#12 - 02/27/2020 11:02 AM - intrigeri
Hi @segfault,

this one is much less urgent than #17477, but it's been waiting for 2 months and maybe you could batch it with that other review.

#13 - 02/29/2020 10:03 PM - segfault
- Status changed from Needs Validation to Resolved
- % Done changed from 0 to 100
Applied in changeset tails/b969a33a961427ae3201b99b1946639368b93ec7.