Meltdown - CVE-2017-5753 CVE-2017-5715 CVE-2017-5754

This article was last updated on: Apr 09, 2018 14:22

IN PROGRESS This article is still under investigation and will be updated as new information is available. Check back often for the most current information.

Background Information
Impact
How to determine if your server is affected
    Determine if you are running CentOS 6 or CentOS 7
    For CloudLinux customers
Resolution
    CentOS 6
    CentOS 7
    For CloudLinux customers
Additional documentation

Background Information

According to Red Hat: "Red Hat has been made aware of multiple microarchitectural (hardware) implementation issues affecting many modern microprocessors, requiring updates to the Linux kernel, virtualization-related components, and/or in combination with a microcode update. An unprivileged attacker can use these flaws to bypass conventional memory security restrictions in order to gain read access to privileged memory that would otherwise be inaccessible. There are 3 known CVEs related to this issue in combination with Intel, AMD, and ARM architectures. Additional exploits for other architectures are also known to exist. These include IBM System Z, POWER8 (Big Endian and Little Endian), and POWER9 (Little Endian)."

Impact

The vulnerability affects all CentOS server versions, and updates are available or planned for supported versions (CentOS 6 and CentOS 7). According to Red Hat: "An industry-wide issue was found with the manner in which many modern microprocessor designs have implemented speculative execution of instructions (a commonly used performance optimization). There are three primary variants of the issue which differ in the way the speculative execution can be exploited. All three rely upon the fact that modern high performance microprocessors implement both speculative execution, and utilize VIPT (Virtually Indexed, Physically Tagged) level 1 data caches that may become allocated with data in the kernel virtual address space during such speculation.

The first two variants abuse speculative execution to perform bounds-check bypass (CVE-2017-5753), or by utilizing branch target injection (CVE-2017-5715) to cause kernel code at an address under attacker control to execute speculatively. Collectively these are known as "Spectre". Both variants rely upon 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 level 1 data cache even for speculatively executed instructions that never actually commit (retire). As a result, an unprivileged attacker could use these two flaws to read privileged memory by conducting targeted cache side-channel attacks. These variants could be used not only to cross syscall boundary (variant 1 and variant 2) but also guest/host boundary (variant 2).

The third variant (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. Researchers have called this exploit "Meltdown". Subsequent memory accesses may cause an allocation into the L1 data cache even when they reference otherwise inaccessible memory locations. As a result, an unprivileged local attacker could read privileged (kernel space) memory (including arbitrary physical memory locations on a host) by conducting targeted cache side-channel attacks."

IMPORTANT: CentOS 5 is not scheduled for updates due to being End Of Life. If you have servers running CentOS 5 we recommend updating to a supported operating system as soon as possible.

How to determine if your server is affected

Determine if you are running CentOS 6 or CentOS 7

You can determine your major CentOS version by running the command below as root:

```
# rpm -q centos-release
```

When running the above command, you will get different results depending on your CentOS version.

For CentOS 6:

```
# rpm -q centos-release
centos-release-6-6.el6.centos.12.2.x86_64
```

If you have confirmed you are running CentOS 6, see the section below.

For CentOS 7:

```
# rpm -q centos-release
centos-release-7-4.1708.el7.centos.x86_64
```

If you have confirmed you are running CentOS 7, see the section below.

For CloudLinux customers

See the following blog post for updates regarding CloudLinux:

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

---

Resolution

cPanel does not distribute the OS packages affected by these vulnerabilities. They are provided by the vendor of the operating system where cPanel & WHM is installed.

CentOS 6

Red Hat has announced the availability of updated packages to address the known vulnerabilities. You can apply the updated packages by running the command below as root:

```
# yum clean all; yum update;
```

You can verify you have an up to date kernel by running the following command as root:

```
# rpm -q kernel | tail -n1
kernel-2.6.32-696.18.7.el6.x86_64
```

The output for the above command should reference kernel version kernel-2.6.32-696.18.7 or later.

NOTE: A reboot is required after updating the kernel unless you have KernelCare configured.

CentOS 7

Red Hat has announced the availability of updated packages to address the known vulnerabilities. You can apply the updated packages by running the command below as root:

```
# yum clean all; yum update;
```

You can verify you have an up to date kernel by running the following command as root:

```
# rpm -q kernel | tail -n1
kernel-3.10.0-693.11.6.el7.x86_64
```

The output for the above command should reference kernel version kernel-3.10.0-693.11.6 or later.

NOTE: A reboot is required after updating the kernel unless you have KernelCare configured.

For CloudLinux customers

See the following blog post for updates regarding CloudLinux:

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

---

Additional documentation

References:

https://access.redhat.com/security/vulnerabilities/speculativeexecution

https://googleprojectzero.blogspot.ca/2018/01/reading-privileged-memory-with-side.html

https://meltdownattack.com/

https://access.redhat.com/articles/3307751

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