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