L1D Flushing

With an increasing number of vulnerabilities being reported around data leaks from the Level 1 Data cache (L1D) the kernel provides an opt-in mechanism to flush the L1D cache on context switch.

This mechanism can be used to address e.g. CVE-2020-0550. For applications the mechanism keeps them safe from vulnerabilities, related to leaks (snooping of) from the L1D cache.

Related CVEs

The following CVEs can be addressed by this mechanism

CVE-2020-0550	Improper Data Forwarding	OS related aspects

Usage Guidelines

Please see document: :ref:`Documentation/userspace-api/spec_ctrl.rst <set_spec_ctrl>` for details.

> **System Message: ERROR/3** (`D:\onboarding-resources\sample-onboarding-resources\linux-master\Documentation\admin-guide\hw-vuln\(linux-master)(Documentation)(admin-guide)(hw-vuln)l1d_flush.rst`, **line 25**); *backlink*
>
> Unknown interpreted text role "ref".

NOTE: The feature is disabled by default, applications need to specifically opt into the feature to enable it.

Mitigation

When PR_SET_L1D_FLUSH is enabled for a task a flush of the L1D cache is performed when the task is scheduled out and the incoming task belongs to a different process and therefore to a different address space.

If the underlying CPU supports L1D flushing in hardware, the hardware mechanism is used, software fallback for the mitigation, is not supported.

Mitigation control on the kernel command line

The kernel command line allows to control the L1D flush mitigations at boot time with the option "l1d_flush=". The valid arguments for this option are:

on	Enables the prctl interface, applications trying to use the prctl() will fail with an error if l1d_flush is not enabled

By default the mechanism is disabled.

Limitations

The mechanism does not mitigate L1D data leaks between tasks belonging to different processes which are concurrently executing on sibling threads of a physical CPU core when SMT is enabled on the system.

This can be addressed by controlled placement of processes on physical CPU cores or by disabling SMT. See the relevant chapter in the L1TF mitigation document: :ref:`Documentation/admin-guide/hw-vuln/l1tf.rst <smt_control>`.

> **System Message: ERROR/3** (`D:\onboarding-resources\sample-onboarding-resources\linux-master\Documentation\admin-guide\hw-vuln\(linux-master)(Documentation)(admin-guide)(hw-vuln)l1d_flush.rst`, **line 62**); *backlink*
>
> Unknown interpreted text role "ref".

NOTE : The opt-in of a task for L1D flushing works only when the task's affinity is limited to cores running in non-SMT mode. If a task which requested L1D flushing is scheduled on a SMT-enabled core the kernel sends a SIGBUS to the task.