Path Spectre и Meltdown OFF
Kernel => 4.15

Для противодействия атаке Meltdown (CVE-2017-5754) на системах x86 с процессорами Intel (процессоры AMD данной атаке не подвержены) добавлена технология PTI (Page Table Isolation), обеспечивающая разделение таблиц страниц памяти ядра и пространства пользователя при переключении контекста во время системного вызова. Для процессоров PowerPC для защиты от Meltdown добавлен код на основе применения инструкции RFI (Return from Interrupt) для сброса кэша L1-D.

Для блокирования эксплуатации второго варианта уязвимости Spectre (CVE-2017-5715) добавлен механизм retpoline, основанный на применении специальной последовательности инструкций, исключающей вовлечение механизма спекулятивного выполнения для косвенных переходов (для работы защиты также требуется сборка модифицированной версией GCC с поддержкой режима "-mindirect-branch=thunk-extern"). Включение средств для обеспечения защиты от первого варианта атаки Spectre (CVE-2017-5753) и кода для блокирования Meltdown на процессорах ARM отложено до выпуска 4.16.

Так как механизмы защиты приводят к снижению производительности, предусмотрены опции для их отключения, которые могут применяться на системах с минимальным риском атаки, например на однопользовательских рабочих станциях. Для отключения PTI во время загрузки ядру можно передать опцию pti=off, а для отключения retpoline - опцию "spectre_v2=off". В состав ядра также добавлен диагностический вызов в sysfs для быстрого определения степени устранения уязвимостей Meltdown и Spectre, который привязан к директории /sys/devices/system/cpu/vulnerabilities/:

$ grep . /sys/devices/system/cpu/vulnerabilities/*

/sys/devices/system/cpu/vulnerabilities/meltdown:Mitigation: PTI

/sys/devices/system/cpu/vulnerabilities/spectre_v1:Vulnerable

/sys/devices/system/cpu/vulnerabilities/spectre_v2:Vulnerable: Minimal generic SM retpoline

Отключение патча:

```
# sudo gedit /etc/default/grub
# GRUB_CMDLINE_LINUX_DEFAULT=»noquiet nosplash pti=off spectre_v2=off»
# sudo update-grub
# sudo reboot
```