Elevation de privilèges

- CVE-2008-(0600|0009|0010) : vmsplice
  - Permet d'exécuter du code sous l'UID 0
    - Versions 2.6.17 à 2.6.24
- CVE-2009-1185 : udev
- CVE-2010-3847 : The GNU C library dynamic linker expands $ORIGIN in setuid library search path
- CVE-2010-3904 : RDS privilege escalation exploit
  - Linux Kernel <= 2.6.36-rc8
- CVE-2013-2094 : Linux kernel perf_swevent_init
  - Linux Kernel < 3.8.9

Exploiter

/usr/share/exploitdb$ ./searchsploit linux kernel local | grep 2.6.3

```
Linux Kernel <= 2.6.3 - (setsockopt) Local Denial of Service Exploit                                | ./linux/dos/274.c
Linux Kernel 2.6.30 <= 2.6.30.1 / SELinux / RHEL5 - Test Kernel Local Root Exploit (0day)           | ./linux/local/9191.txt
Linux Kernel <= 2.6.31-rc5 sigaltstack 4-Byte Stack Disclosure Exploit                              | ./linux/local/9352.c
Linux Kernel <= 2.6.31-rc7 AF_LLC getsockname 5-Byte Stack Disclosure                               | ./linux/local/9513.c
Linux Kernel <= 2.6.30 atalk_getname() 8-bytes Stack Disclosure Exploit                             | ./linux/local/9521.c
Linux Kernel < 2.6.31-rc7 - AF_IRDA 29-Byte Stack Disclosure Exploit                                | ./linux/local/9543.c
Linux Kernel 2.4.1-2.4.37 and 2.6.1-2.6.32-rc5 - Pipe.c Privilege Escalation                        | ./linux/local/9844.py
Linux Kernel <= 2.6.34-rc3 ReiserFS xattr - Privilege Escalation                                    | ./linux/local/12130.py
Linux Kernel < 2.6.36-rc1 CAN BCM - Privilege Escalation Exploit                                    | ./linux/local/14814.c
Linux Kernel < 2.6.36-rc4-git2 - x86_64 ia32syscall Emulation Privilege Escalation                  | ./linux/local/15023.c
Linux Kernel 2.6.27 < 2.6.36 - x86_64 compat Local Root Exploit                                     | ./linux/local/15024.c
Linux Kernel < 2.6.36-rc6 pktcdvd Kernel Memory Disclosure                                          | ./linux/local/15150.c
Linux Kernel <= 2.6.36-rc8 - RDS Protocol Local Privilege Escalation                                | ./linux/local/15285.c
Linux Kernel <= 2.6.37 - Local Privilege Escalation                                                 | ./linux/local/15704.c
Linux Kernel < 2.6.37-rc2 - ACPI custom_method Privilege Escalation                                 | ./linux/local/15774.c
Linux Kernel 2.6.34 - CAP_SYS_ADMIN x86 - Local Privilege Escalation Exploit                        | ./linux/local/15916.c
Linux Kernel < 2.6.34 - CAP_SYS_ADMIN x86 & x64 - Local Privilege Escalation Exploit (2)            | ./linux/local/15944.c
Linux Kernel <= 2.6.37 - Local Kernel Denial of Service                                             | ./linux/dos/16263.c
Linux Kernel < 2.6.36.2 - Econet Privilege Escalation Exploit                                       | ./linux/local/17787.c
Linux Kernel <= 2.6.37-rc1 - serial_multiport_struct Local Info Leak Exploit                        | ./linux/local/18080.c
Linux Kernel 2.6.39 <= 3.2.2 (32-bit & 64-bit) - Mempodipper Local Root (1)                         | ./linux/local/18411.c
Linux Kernel 2.6.37 <= 3.x.x - PERF_EVENTS Local Root Exploit                                       | ./linux/local/25444.c
Linux Kernel 2.6.x - Audit Subsystems Local Denial of Service Vulnerability                         | ./linux/dos/29683.txt
Linux Kernel 2.6.31 - 'perf_counter_open()' Local Buffer Overflow Vulnerability                     | ./linux/local/33228.txt
Linux Kernel <= 2.6.39 (32-bit & 64-bit) - Mempodipper Local Root (2)                               | ./linux/local/35161.txt
```