
Posted by [seyko2](#) on Thu, 07 Jun 2007 03:47:17 GMT

[View Forum Message](#) <> [Reply to Message](#)

Posted by [dev](#) on Thu, 07 Jun 2007 10:52:39 GMT

[View Forum Message](#) <> [Reply to Message](#)

<http://download.openvz.org/~dev/patch-028stab034-core>

Posted by [seyko2](#) on Thu, 07 Jun 2007 23:36:30 GMT

[View Forum Message](#) <> [Reply to Message](#)

```

Freeing SMP alternatives: 16k freed
Page beancounter hash is 16384 entries.
Brought up 1 CPUs
checking if image is initramfs... it is
Freeing initrd memory: 3122k freed
list_add corruption. prev->next should be c068bd6c, but was c0ad987c
-----[ cut here ]-----
kernel BUG at lib/list_debug.c:31!
invalid opcode: 0000 [#1]
SMP
last sysfs file:
Modules linked in:
CPU: 0, VCPU: 0.0
EIP: 0061:[<c04d5e14>] Not tainted VLI
EFLAGS: 00010046 (2.6.18-fan_rh5_openvz_xen-028.034 #1)
EIP is at __list_add+0x3c/0x58
eax: 00000048 ebx: c068bd6c ecx: c0ac5e44 edx: c0ac5e44
esi: c0ad926c edi: c0ad8c5c ebp: c0ad8660 esp: c0ac5e40
ds: 007b es: 007b ss: e021
Process swapper (pid: 1, veid: 0, ti=c0ac4000 task=c0ad9890 task.ti=c0ac4000)
Stack: c0646b70 c068bd6c c0ad987c 00000000 c0adee08 c0ade8c8 c041bcf9 00000004
00000004 c0ac5ee0 00000000 00800711 c0ac5ee0 c0ae04a4 ffffffff 00800711
c041bfd1 00000000 00000000 00000000 c0ae04a4 00000000 00000000 c068d080
Call Trace:
[<c041bcf9>] copy_process+0xc66/0xe77
[<c041bfd1>] do_fork_pid+0x6e/0x16b
[<c04543c4>] buffered_rmqueue+0x105/0x122
[<c0430d2b>] kthread+0x0/0x9f
[<c041c0f2>] do_fork+0x13/0x17
[<c0402c72>] kernel_thread+0xa3/0xad
[<c0430d2b>] kthread+0x0/0x9f
[<c0402bc4>] kernel_thread_helper+0x0/0xb
[<c0430ddf>] keventd_create_kthread+0x15/0x4f
[<c0430e95>] kthread_create+0x7c/0xba
[<c0430dca>] keventd_create_kthread+0x0/0x4f
[<c042dbde>] worker_thread+0x0/0x138
[<c042dea2>] create_workqueue_thread+0x79/0x90
[<c042dbde>] worker_thread+0x0/0x138
[<c042df5b>] __create_workqueue+0xa2/0xe9
[<c0402067>] init+0x0/0x141
[<c042e218>] init_workqueues+0x1b/0x33
[<c070e9b9>] do_basic_setup+0xf/0x23
init+0x51/0x14

```

Posted by [seyko2](#) on Fri, 08 Jun 2007 04:17:59 GMT

[View Forum Message](#) <> [Reply to Message](#)

Posted by [seyko2](#) on Fri, 08 Jun 2007 06:14:28 GMT

[View Forum Message](#) <> [Reply to Message](#)

Posted by [dev](#) on Fri, 08 Jun 2007 07:45:17 GMT
[View Forum Message](#) <> [Reply to Message](#)

Posted by [dev](#) on Fri, 08 Jun 2007 08:05:57 GMT
[View Forum Message](#) <> [Reply to Message](#)

Posted by [dev](#) on Fri, 08 Jun 2007 08:25:05 GMT
[View Forum Message](#) <> [Reply to Message](#)

patch 1:

```
--- ./kernel/ve/veowner.c.ve2505 2007-06-07 12:43:15.000000000 +0400
+++ ./kernel/ve/veowner.c 2007-06-08 12:21:09.000000000 +0400
@@ -237,20 +237,6 @@ void init_ve_system(void)
```

```

ve = get_ve0();

- /* Don't forget about idle tasks */
- write_lock_irqsave(&tasklist_lock, flags);
- for (i = 0; i < NR_CPUS; i++) {
-   tsk = idle_task(i);
-   if (tsk == NULL)
-     continue;
-
-   prepare_ve0_process(tsk);
- }
- do_each_thread_all(p, tsk) {
-   prepare_ve0_process(tsk);
- } while_each_thread_all(p, tsk);
- write_unlock_irqrestore(&tasklist_lock, flags);
-
init_entry = child_reaper;
ve->init_entry = init_entry;
/* if ve_move_task to VE0 (e.g. in cpt code) */

```

patch2:

```

--- a/net/sunrpc/sched.c
+++ b/net/sunrpc/sched.c
@@ -996,12 +996,12 @@ fail:

void rpc_run_child(struct rpc_task *task, struct rpc_task *child, rpc_action func)
{
- rpc_set_active(task);
+ rpc_set_active(child);

spin_lock_bh(&childq.lock);
/* N.B. Is it possible for the child to have already finished? */
__rpc_sleep_on(&childq, task, func, NULL);
- rpc_make_runnable(task);
+ rpc_make_runnable(child);
spin_unlock_bh(&childq.lock);
}

```

Posted by [dev](#) on Fri, 08 Jun 2007 08:32:09 GMT
[View Forum Message](#) <> [Reply to Message](#)

fixed patch-028stab034-core uploaded to the same URL

Posted by [seyko2](#) on Sat, 09 Jun 2007 04:11:54 GMT

[View Forum Message](#) <> [Reply to Message](#)

ddcxinfo-knoppix -monitor

Posted by [dev](#) on Sat, 09 Jun 2007 07:40:38 GMT

[View Forum Message](#) <> [Reply to Message](#)

Posted by [seyko2](#) on Sun, 10 Jun 2007 05:31:30 GMT

[View Forum Message](#) <> [Reply to Message](#)

```
extern void kernel_thread_helper(void);
EXPORT_SYMBOL(kernel_thread_helper);
+ __asm__(".section .text\n"
+        ".align 4\n"
+        ".global kernel_thread_helper\n"
+        "kernel_thread_helper:\n\t"
+        "movl %edx,%eax\n\t"
+        "pushl %edx\n\t"
+        "call *%ebx\n\t"
+        "pushl %eax\n\t"
+        "call do_exit\n\t"
+        ".previous");
```

```
diff -urN linux-2.6.18-openvzelx-028.030-orig/arch/i386/kernel/traps-xen.c
linux-2.6.18-openvzelx-028.030/arch/i386/kernel/t
--- linux-2.6.18-openvzelx-028.030-orig/arch/i386/kernel/traps-xen.c    2007-04-24
18:19:31.000000000 +0400
+++ linux-2.6.18-openvzelx-028.030/arch/i386/kernel/traps-xen.c 2007-04-24
18:20:05.000000000 +0400
@@ -748,6 +748,14 @@
```

```
static DEFINE_SPINLOCK(nmi_print_lock);

+#ifdef CONFIG_SMP
+int __attribute__((weak))
+smp_nmi_call_function(smp_nmi_function func, void *info, int wait)
+{
+    return 0;
+}
+#endif
+
void die_nmi (struct pt_regs *regs, const char *msg)
```

```
{  
    if (notify_die(DIE_NMIWATCHDOG, msg, regs, 0, 2, SIGINT) ==
```

<http://89.19.167.91/fantoo/patch-028stab034-core.ver02.addon>

028.034

Posted by [seyko2](#) on Mon, 11 Jun 2007 04:12:31 GMT

[View Forum Message](#) <> [Reply to Message](#)

<http://89.19.167.91/fantoo/028.034-git.patch>

```
diff -urN linux-2.6.18-028.034.git/net/sunrpc/clnt.c linux-2.6.18-028.034/net/sunrpc/clnt.c  
--- linux-2.6.18-028.034.git/net/sunrpc/clnt.c 2007-06-11 03:57:23.000000000 +0400  
+++ linux-2.6.18-028.034/net/sunrpc/clnt.c 2007-06-11 07:26:47.000000000 +0400  
@@ -299,9 +299,7 @@  
     new->cl_autobind = 0;  
     new->cl_oneshot = 0;  
     new->cl_dead = 0;
```

```
- new->cl_broken = 0;
- if (!IS_ERR(new->cl_dentry))
-     dget(new->cl_dentry);
+ new->cl_broken = 0;
  rpc_init_rtt(&new->cl_rtt_default, clnt->cl_xprt->timeout.to_initval);
  if (new->cl_auth)
      atomic_inc(&new->cl_auth->au_count);
```

!IS_ERR

Posted by [seyko2](#) on Mon, 11 Jun 2007 05:09:32 GMT

[View Forum Message](#) <> [Reply to Message](#)

ddcxinfo-knoppix -monitor

(!IS_ERR(new->cl_dentry)))

Posted by [seyko2](#) on Tue, 12 Jun 2007 03:37:04 GMT

[View Forum Message](#) <> [Reply to Message](#)

```
--- arch/i386/kernel/vm86.c.old 2007-06-12 06:05:00.000000000 +0400
+++ arch/i386/kernel/vm86.c    2007-06-12 06:11:17.000000000 +0400
@@ -125,11 +125,15 @@
```

```

    }

#ifdef CONFIG_X86_NO_TSS
-   tss = &per_cpu(init_tss, get_cpu());
+   tss = __get_cpu_tss(get_cpu());
#endif
    current->thread.esp0 = current->thread.saved_esp0;
    current->thread.sysenter_cs = __KERNEL_CS;
#ifdef CONFIG_X86_NO_TSS
+   load_virtual_esp0(tss, current);
#else
    load_esp0(tss, &current->thread);
#endif
    current->thread.saved_esp0 = 0;
#ifdef CONFIG_X86_NO_TSS
    put_cpu();
@@ -305,14 +309,17 @@
    savesegment(gs, tsk->thread.saved_gs);

#ifdef CONFIG_X86_NO_TSS
-   tss = &per_cpu(init_tss, get_cpu());
+   tss = __get_cpu_tss(get_cpu());
#endif
    tsk->thread.esp0 = (unsigned long) &info->VM86_TSS_ESP0;
    if (cpu_has_sep)
        tsk->thread.sysenter_cs = 0;
-   load_esp0(tss, &tsk->thread);
+
#ifdef CONFIG_X86_NO_TSS
+   load_virtual_esp0(tss, tsk);
    put_cpu();
#else
+   load_esp0(tss, &tsk->thread);
#endif

    tsk->thread.screen_bitmap = info->screen_bitmap;

```

Posted by [seyko2](#) on Tue, 12 Jun 2007 14:55:52 GMT
[View Forum Message](#) <> [Reply to Message](#)

Posted by [dev](#) on Wed, 13 Jun 2007 07:46:33 GMT
[View Forum Message](#) <> [Reply to Message](#)

```
ENTRY(kernel_thread_helper)
    pushl $0          # fake return address for unwinder
    CFI_STARTPROC
    movl %edx,%eax
    push %edx
    CFI_ADJUST_CFA_OFFSET 4
    call *%ebx
    push %eax
    CFI_ADJUST_CFA_OFFSET 4
    call do_exit
    CFI_ENDPROC
ENDPROC(kernel_thread_helper)
```

```
#ifndef CONFIG_X86_NO_TSS
-   tss = &per_cpu(init_tss, get_cpu());
+   tss = __get_cpu_tss(get_cpu());
#endif

--- ./arch/i386/kernel/vm86.c.ve2555  2007-06-08 19:38:56.000000000 +0400
+++ ./arch/i386/kernel/vm86.c  2007-06-13 12:26:23.000000000 +0400
@@ -129,9 +129,7 @@ struct pt_regs * fastcall save_v86_state
#endif
    current->thread.esp0 = current->thread.saved_esp0;
    current->thread.sysenter_cs = __KERNEL_CS;
-#ifndef CONFIG_X86_NO_TSS
    load_virtual_esp0(tss, current);
-#endif
    current->thread.saved_esp0 = 0;
#ifndef CONFIG_X86_NO_TSS
    put_cpu();
@@ -313,8 +311,8 @@ static void do_sys_vm86(struct kernel_vm
    if (cpu_has_sep)
        tsk->thread.sysenter_cs = 0;

-#ifndef CONFIG_X86_NO_TSS
    load_virtual_esp0(tss, tsk);
+#ifndef CONFIG_X86_NO_TSS
    put_cpu();
#endif
```

Posted by [dev](#) on Wed, 13 Jun 2007 08:35:04 GMT
[View Forum Message](#) <> [Reply to Message](#)

Quote:

Quote:

Posted by [dev](#) on Wed, 13 Jun 2007 08:44:24 GMT
[View Forum Message](#) <> [Reply to Message](#)

```
diff -u include/asm/mach-xen/asm/processor.h.orig include/asm/mach-xen/asm/processor.h
--- include/asm/mach-xen/asm/processor.h.orig 2007-06-14 00:15:55.000000000 +0400
+++ include/asm/mach-xen/asm/processor.h 2007-06-14 00:16:07.000000000 +0400
@@ -569,6 +569,32 @@
 */
extern int kernel_thread(int (*fn)(void *), void * arg, unsigned long flags);

#ifdef CONFIG_X86_HIGH_ENTRY
#define virtual_esp0(task) \
+ ((unsigned long)((task)->thread_info->virtual_stack + ((task)->thread.esp0 - (unsigned
long)(task)->thread_info->real_stack)))
#define load_virtual_esp0(tss, task) \
+ do { \
+     tss->esp0 = virtual_esp0(task); \
+     if (likely(cpu_has_sep) && unlikely(tss->ss1 != (task)->thread.sysenter_cs)) { \
+         tss->ss1 = (task)->thread.sysenter_cs; \
+         wrmsr(MSR_IA32_SYSENTER_CS, \
+             (task)->thread.sysenter_cs, 0); \
+     } \
+ } while (0)
+
#else
#define virtual_esp0(task) ((task)->thread.esp0)
#define load_virtual_esp0(tss, task) load_esp0(tss, &(task)->thread)
+
#endif
+
#ifdef CONFIG_XEN
#define __get_cpu_tss(cpu) (init_tss + (cpu))
#else
#define __get_cpu_tss(cpu) (&per_cpu(init_tss, cpu))
#endif
+
extern unsigned long thread_saved_pc(struct task_struct *tsk);
void show_trace(struct task_struct *task, struct pt_regs *regs, unsigned long *stack);
```

desc.h
fixmap.h
highmem.h
kmap_types.h
mmu.h
mmu_context.h
page.h
pgtable.h
processor.h
system.h
tlbflush.h

Posted by [dev](#) on Thu, 14 Jun 2007 11:25:13 GMT
[View Forum Message](#) <> [Reply to Message](#)

include/asm/processor.h

Quote:

```
diff -u include/asm/mach-xen/asm/processor.h.orig include/asm/mach-xen/asm/processor.h
--- include/asm/mach-xen/asm/processor.h.orig 2007-06-14 00:15:55.000000000 +0400
+++ include/asm/mach-xen/asm/processor.h 2007-06-14 00:16:07.000000000 +0400
@@ -569,6 +569,32 @@
```

```
    */
extern int kernel_thread(int (*fn)(void *), void * arg, unsigned long flags);

#ifdef CONFIG_X86_HIGH_ENTRY
#define virtual_esp0(task) \
+ ((unsigned long)((task)->thread_info->virtual_stack + ((task)->thread.esp0 - (unsigned \
long)(task)->thread_info->real_stack)))
#define load_virtual_esp0(tss, task) \
+ do { \
+     tss->esp0 = virtual_esp0(task); \
+     if (likely(cpu_has_sep) && unlikely(tss->ss1 != (task)->thread.sysenter_cs)) { \
+         tss->ss1 = (task)->thread.sysenter_cs; \
+         wrmsr(MSR_IA32_SYSENTER_CS, \
+             (task)->thread.sysenter_cs, 0); \
+     } \
+ } while (0)
+
#else
+
#define virtual_esp0(task) ((task)->thread.esp0)
#define load_virtual_esp0(tss, task) load_esp0(tss, &(task)->thread)
+
#endif
+
#ifdef CONFIG_XEN
#define __get_cpu_tss(cpu) (init_tss + (cpu))
#else
#define __get_cpu_tss(cpu) (&per_cpu(init_tss, cpu))
#endif
+
extern unsigned long thread_saved_pc(struct task_struct *tsk);
void show_trace(struct task_struct *task, struct pt_regs *regs, unsigned long *stack);
```

```
--- ./arch/i386/Kconfig.ve9992 2007-06-08 19:39:07.000000000 +0400
+++ ./arch/i386/Kconfig 2007-06-14 14:58:27.000000000 +0400
@@ -223,6 +223,7 @@ source "arch/i386/Kconfig.cpu"
```

config X86_4G

```

    bool "4 GB kernel-space and 4 GB user-space virtual memory support"
+   depends on !X86_XEN
    help
        This option is only useful for systems that have more than 1 GB
        of RAM.
--- ./include/asm-i386/mach-xen/asm/processor.h.ve9992 2007-06-08 19:39:07.000000000
+0400
+++ ./include/asm-i386/mach-xen/asm/processor.h 2007-06-14 15:04:30.000000000 +0400
@@ -535,6 +535,9 @@ static inline void __load_esp0(struct ts
    HYPERVISOR_stack_switch(__KERNEL_DS, (thread)->esp0)
#endif

+#define load_virtual_esp0(tss, task) load_esp0(tss, &(task)->thread)
+#define __get_cpu_tss(cpu) (&per_cpu(init_tss, cpu))
+
#define start_thread(regs, new_eip, new_esp) do {      \
    __asm__("movl %0,%%fs ; movl %0,%%gs": : "r" (0)); \
    set_fs(USER_DS);                                  \

```

Quote:

```

desc.h
fixmap.h
highmem.h
kmap_types.h
mmu.h
mmu_context.h
page.h
pgtable.h
processor.h
system.h
tlbflush.h

```

Quote:

<http://download.openvz.org/~dev/patches-035-ovz/>

Quote:

Posted by [seyko2](#) on Thu, 14 Jun 2007 14:29:58 GMT
[View Forum Message](#) <> [Reply to Message](#)

Posted by [dev](#) on Thu, 14 Jun 2007 14:34:40 GMT

[View Forum Message](#) <> [Reply to Message](#)

Posted by [dev](#) on Thu, 14 Jun 2007 18:42:44 GMT

[View Forum Message](#) <> [Reply to Message](#)

https://wiki.openvz.org/How_to_use_OpenVZ_as_a_XEN_guest_OS_%28for_x86_platform%29

Posted by [seyko2](#) on Thu, 14 Jun 2007 19:14:08 GMT

[View Forum Message](#) <> [Reply to Message](#)

EXT3-fs: mounted filesystem with ordered data mode.

4gb seg fixup, process init (pid 1), cs:ip 73:00a2c760

4gb seg fixup, process init (pid 1), cs:ip 73:00a2c760

4gb seg fixup, process init (pid 1), cs:ip 73:00aa1b69

4gb seg fixup, process init (pid 1), cs:ip 73:00a2fd5c

4gb seg fixup, process init (pid 1), cs:ip 73:00a2fd6a

4gb seg fixup, process init (pid 1), cs:ip 73:00a2fd5c

4gb seg fixup, process init (pid 1), cs:ip 73:00a2fd6a

4gb seg fixup, process init (pid 1), cs:ip 73:009eab7b

4gb seg fixup, process init (pid 1), cs:ip 73:009eab64

4gb seg fixup, process init (pid 1), cs:ip 73:00a358b5

printk: 109680 messages suppressed.

4gb seg fixup, process hwclock (pid 276), cs:ip 73:0052c480

4gb seg fixup, process hwclock (pid 276), cs:ip 73:490ce6f6

4gb seg fixup, process hwclock (pid 276), cs:ip 73:005b00c8

printk: 567140 messages suppressed.

4gb seg fixup, process S14nfslock (pid 2477), cs:ip 73:0090a85e

printk: 705301 messages suppressed.

4gb seg fixup, process modprobe (pid 2671), cs:ip 73:00bd7811

printk: 555473 messages suppressed.

4gb seg fixup, process S90xfs (pid 2823), cs:ip 73:0071185e

EXT3-fs: mounted filesystem with ordered data mode.

4gb seg fixup, process init (pid 1), cs:ip 73:00cbf760

4gb seg fixup, process init (pid 1), cs:ip 73:00d34b69

4gb seg fixup, process init (pid 1), cs:ip 73:00cc2d5c

4gb seg fixup, process init (pid 1), cs:ip 73:00cc2d6a

4gb seg fixup, process init (pid 1), cs:ip 73:00cc2d5c

4gb seg fixup, process init (pid 1), cs:ip 73:00cc2d5c

4gb seg fixup, process init (pid 1), cs:ip 73:00cc2d6a

4gb seg fixup, process init (pid 1), cs:ip 73:00c7db7b

4gb seg fixup, process init (pid 1), cs:ip 73:00c7db64

4gb seg fixup, process init (pid 1), cs:ip 73:00cc88b5

printk: 109695 messages suppressed.

4gb seg fixup, process hwclock (pid 276), cs:ip 73:00506480

4gb seg fixup, process hwclock (pid 276), cs:ip 73:490ce6f6

4gb seg fixup, process hwclock (pid 276), cs:ip 73:0058a0c8

Posted by [seyko2](#) on Fri, 15 Jun 2007 05:51:08 GMT
[View Forum Message](#) <> [Reply to Message](#)

Posted by [seyko2](#) on Fri, 15 Jun 2007 06:53:45 GMT
[View Forum Message](#) <> [Reply to Message](#)

Quote:OpenVZ XenLinux kernel is able to work also in Dom0. It can be tested just by updating /etc/grub.conf on the hardware node. But in this case it will be impossible to start DomUs. It is a known bug and it is related not to OpenVZ, but to RHEL5 kernel.

Posted by [seyko2](#) on Fri, 15 Jun 2007 07:36:01 GMT
[View Forum Message](#) <> [Reply to Message](#)

Posted by [dev](#) on Fri, 15 Jun 2007 10:02:00 GMT
[View Forum Message](#) <> [Reply to Message](#)

```
#define __USER_CS (GDT_ENTRY_DEFAULT_USER_CS * 8 + 3)
```

diff list-028stab027 list-028stab037

3c3,13

< # Based on 2.6.18-8.1.1.el5 kernel

> # Based on 2.6.18-8.1.4.el5 kernel

>

> # -----

> # 4gb split

> diff-arch-4gb-20070409-2

> diff-arch-4gb-cr4-20070410 # to LKML

> diff-arch-x86-ioremap-guard-page-fix-20070419

> diff-arch-4gb-ldt-irqs-20070515

> diff-arch-4gb-xen-20070523

> diff-arch-4gb-xen-cleanup-20070528

> diff-arch-4gb-xen-b-20070613

23a34

> namespaces-utsname-xen.patch

46a58

> io-accounting-menuconfig.patch

71a84

> diff-ms-cpufreq-centrino-20070426

78a92,94

> diff-ms-cfq-allow-merge-b-20070424

> diff-ms-cfq-allow-merge-c-20070507

> diff-ms-cfq-rm-redundant-find-next-req-20070509

91a108,110

> diff-ms-ext3-iread-brelse-20070601

> diff-ms-ext3-orhpan-list-corruption-20070531

> diff-ms-ext3-orhpan-list-corruption-b-20070603

93a113,147

> diff-ms-lockdep-neighbour-table-class-20070409

> diff-ms-bridge-unaligned-access-20070411 # send to LKML

> diff-ms-stopmachine-msleep-20070411 # send to LKML

> diff-ms-elf-retval-20070420 # send to LKML

> diff-ms-loop-dont-complete-lo-bh-done-20070418

> # diff-ms-fib-netlink-lookup-recursion-20070425

> # diff-ms-fib-netlink-lookup-recursion-b-20070425

> # `linux-2.6-net-fix-user-oops-able-bug-in-fib-netlink.patch

> diff-ms-slab-numa-bind-20070514

> diff-ms-futex-locking-bug-20070510

> diff-ms-futex-oops-20070510

> diff-ms-nfs-rm-warn-20070515

```

> diff-ms-sparc64-compilation-20070523
> diff-ms-powerpc-compilation-20070523
> diff-ms-nfs-odirect-20070529
> diff-ms-nfs-umount-refcnt-leak-20070530
> diff-ms-nfs-schedlock-20070530
> diff-ms-nfs-laundry-20070530
> diff-ms-seqfile-seek-20070601
> diff-ms-ia64-nat-ptrace-20070604
> diff-ms-net-ipv6-privacy-msg-20070605
> diff-ms-entropy-fix-a-20070530      # CVE-2007-2453
> diff-ms-entropy-fix-b-20070530      # CVE-2007-2453
> diff-ms-security-cpuset-20070605    # CVE-2007-2875
> diff-ms-security-sctp-20070604      # CVE-2007-2876
>>
> diff-ms-fuse-nlookup-20070521
> diff-ms-fuse-spurious-bug-20070521
> diff-ms-fuse-dentry-parent-20070521
> diff-ms-fuse-oops-in-lookup-20070521
> diff-ms-fuse-bug-control-fs-20070521
> diff-ms-fuse-validate-rootmode-20070521
> diff-ms-fuse-mknod-of-regular-file-20070521
>
> # diff-ms-fatal-signal-20070413
108c162
< diff-bug-macro-tune-20060310      # Send to LKML
---
> diff-bug-macro-tune-20060310-2      # Send to LKML
134a189
> diff-sysrq-debug-b-20070511
159a215
> diff-rh-mmap-return-addr-b-20070608
170a227
> diff-ms-vfs-get-host-20070515
174c231,232
< diff-ms-nmi-wdog-timeout-20070328
---
> # diff-ms-nmi-wdog-timeout-20070328
> # `linux-2.6-nmi-change-watchdog-timeout-to-30-seconds.patch
178,179c236,237
< diff-ms-net-bridge-via-eth-20070311
< diff-rh-utrace-update-20070320
---
> # diff-rh-utrace-update-20070320
> # `linux-2.6-utrace-exploit-and-unkillable-cpu-fixes.patch
180a239,240
> diff-rh-dlm-misc-device-fix-20070412
> diff-ms-bridge-nf-ebt-among-20070607
189d248

```

```

< # diff-ve-sysctl-allow-kthreads-20061018
224c283
< diff-ubc-kmem-20060830-3
---
> diff-ubc-kmem-20060830-4
349a409,425
> diff-ubc-refcount-leak-dupmm-20070409
> diff-ubc-vmguar-enough-null-mm-20070406
> diff-ubc-page-uncharge-bug-first-20070406
> diff-ubc-percpu-sign-expansion-20070410
> diff-ubc-dcache-uncharge-root-20070413
> diff-ubc-put-beancounters-in-fork-20070416
> diff-ubc-io-release-debug-20070416
> diff-ubc-unusedprivvm-in-zeromap-20070424
> diff-ubc-off-20070424
> diff-ubc-dentry-acentry-20070510
> diff-ubc-dentry-free_block-20070510
> diff-ubc-dentry-free_alien-20070510
> diff-ubc-dentry-free_alien-b-20070521
> diff-ubc-cleanup-20070517

> diff-ubc-proc-rework-b-20070515
> diff-ubc-proc-rework-c-20070604
> diff-ubc-unix-exports-20070604
379a456,464
> diff-ubc-ioprio-clean-active-ub-20070411
> diff-ubc-ioprio-oops-on-virt-off-20070423
> diff-ubc-ioprio-force-disp-off-20070424
> diff-ubc-ioprio-range-prio-20070623
> diff-ubc-ioprio-slice-scaling-20070623
> diff-ubc-ioprio-on-dispatch-check-20070523
>
> diff-ubc-ioacct-context-handle-20070413
> diff-ubc-top-beancounter-20070515
427a513
> diff-ve-meminfo-b-20070330
506a593
> diff-ve-futex-vpid-fix-20070413
520c607
< diff-ve-sysctl-allow-kthreads-20061018
---
> diff-ve-sysctl-allow-kthreads-20061018-2
573a661
> diff-ve-tun-persist-20070424
602a691,708
> diff-ve-kconfig-security-deps-20070411
> diff-ve-netlink-veprintk-20070426
> diff-ve-xen-netback-20070426

```

> diff-ve-pid-nr-fix-20070503
> diff-ve-showmem-locking-20070414
> diff-ve-init-signals-20070514
> diff-ve-proc-hash-pid-dentries-20070516
> diff-ve-cap-bset-20070504
> diff-ve-net-arp-set-perms-20070625
> diff-ve-cpustats-20070528
> diff-ve-setattr-proc-20070524
> diff-ve-setattr-proc-kmsg-20070524
> diff-ve-setattr-proc-b-20070604
> diff-ve-syslog-20070601
> diff-ve-reparent-threaded-init-20070604
> diff-ve-vpsdumpable-early-20070604
> diff-ve-oom-adjust-20070604
> diff-ve-prepare-ve0-tasks-20070608
626a733,736
> diff-ve-venet-stoprace-20070412
> diff-ve-net-veth-addr-macro-20070514
> diff-ve-net-veth-multicast-20070604
> diff-ve-net-veth-filtering-b-20070605
640a751,756
> diff-ve-nfs-hostcache-20070510
> diff-ve-nfs-stop-20070502
> diff-ve-nfs-stop-b-20070502
> diff-ve-nfs-abortset-20070504
> diff-ve-nfs-tcpabort-20070522
> diff-ve-nfs-abortcorrupt-20070523
665a782,784
> diff-ve-nf-iptables-aliasing-20070515
> diff-ve-ip-nat-aliasing-20070605
> diff-ve-ip-nat-aliasing-b-20070607
680a800,804
> # bridges over ETH
> diff-ms-net-bridge-via-eth-20070311
> diff-ve-net-bridge-via-phys-dev2-20070514
> diff-ms-net-bridge-via-eth-c-20070613
>
717a842,849
> diff-vzdq-sleep-under-inode-lock-20070412
> diff-vzdq-ugbad-20070428
> diff-vzdq-ppc32-comp-20070518
> diff-vzdq-putsuper-20070518
> diff-vzdq-aquota-group-len-20070521
> diff-vzdq-atomic-in-buildmntlist-20070521
> diff-vzdq-for-gfs-20070521
> diff-vzdq-restore-symlinks-under-sem-20070524
723c855
< diff-cpt-exports-4

> diff-cpt-exports-5
770a903
> diff-cpt-inotify-core-b-20070529
842a976
> diff-cpt-kill-external-processes-b-20070515
852a987
> diff-cpt-ubc-adjust-on-restore-c-20070601
863a999,1000
> diff-cpt-4gbsplit-ldt-20070410
> diff-cpt-off-lockdep-on-sockets-20070413
868a1006,1035
> diff-cpt-make-zombie-20070413
> diff-cpt-make-zombie-b-20070420
> diff-cpt-zombie-threads-20070416
> diff-cpt-robust-list-20070413
> diff-cpt-active-callback-eagain-20070423
> diff-cpt-restore-netlink-socket-20070419
> diff-cpt-suspend-cleanup-20070510
> diff-cpt-prevent-vm-changes-20070510
> diff-cpt-features-known-mask-20070514
> diff-cpt-futex-eintr-20070510
> diff-cpt-cap-bset-20070504
> diff-cpt-xen-ldt-20070523
> diff-cpt-wait-fix-20070518
> diff-cpt-wait-fix-b-20070518
> diff-cpt-wait-fix-c-20070601
> diff-cpt-mm-deadlock-20070523
> diff-cpt-restore-lastpid-20070604
> diff-cpt-pids-leak-20070525
> diff-cpt-rst-file-error-msg-20070601
> diff-cpt-namespace-deadlock-20070604
> diff-cpt-ia64-nat-20070604
> diff-cpt-improve-align-20070604
> diff-cpt-compilation-warning-20070604
> diff-cpt-ia64-unaligned-suppress-20070604
> diff-cpt-check-iptables-modules-20070604
> diff-cpt-restore-deleted-files-20070502
> diff-cpt-deleted-ref-20070502
> diff-cpt-deleted-ref-b-20070613
> diff-cpt-restore-packet-socket-20070606
>
870a1038,1040
> # Required for VZ only:
> diff-cpt-aux-task-list-20070604
>
890a1061
> diff-fairsched-ppc-syscalls-fix3-20070525

```
910c1081
< diff-fairsched-get-normal-vemask-20061220
---
> diff-fairsched-get-normal-vemask-20061220-2
922a1094
> diff-fairsched-find-idle-vcpu-20070403
925a1098,1099
> diff-fairsched-best-vcpu-20070413
> diff-fairsched-best-vcpu-b-20070423
928a1103,1111
> diff-fairsched-unused-rq-20070424
> diff-fairsched-dyn-vcpu-timeslice-20070518
> diff-fairsched-vcpuoff-comp-20070426
> diff-fairsched-rename-vcpu-info-20070517
> diff-fairsched-x8664-show-regs-20070528
> diff-fairsched-boot-cpu-20070530
> diff-fairsched-preempt-20070529
> diff-fairsched-iowait-fix-20070624
> diff-fairsched-tickduration-20070528
931a1115,1122
>
> diff-ms-dcache-fix-quadratic-shrink
> diff-ubc-move-might-sleep-20070517
>
> # Xen fixes here and there...
> diff-ve-xen-blktapmain-20070514
> diff-xen-subarch-changes-20070528
> diff-ms-net-settimeout-20070525
```

[/code]

Posted by [dev](#) on Fri, 15 Jun 2007 10:09:04 GMT

[View Forum Message](#) <> [Reply to Message](#)

```
struct desc_struct default_ldt[] = { { 0, 0 }, { 0, 0 }, { 0, 0 },
                                       { 0, 0 }, { 0, 0 } };
```

Posted by [dev](#) on Fri, 15 Jun 2007 10:10:29 GMT

[View Forum Message](#) <> [Reply to Message](#)

Posted by [seyko2](#) on Fri, 15 Jun 2007 11:08:18 GMT

[View Forum Message](#) <> [Reply to Message](#)

```
--- ./fs/exec.c.ve254 2006-08-29 10:47:09.000000000 +0400
+++ ./fs/exec.c 2006-08-29 10:47:09.000000000 +0400
@@ -66,6 +66,8 @@ int suid_dumpable = 0;
EXPORT_SYMBOL(suid_dumpable);
/* The maximal length of core_pattern is also specified in sysctl.c */

+int sysctl_at_vsyscall;
+
static struct linux_binfmt *formats;
static DEFINE_RWLOCK(binfmt_lock);

--- ./include/asm-i386/elf.h.ve254 2006-08-29 10:47:08.000000000 +0400
+++ ./include/asm-i386/elf.h 2006-08-29 10:47:54.000000000 +0400
@@ -162,7 +162,7 @@ extern int arch_setup_additional_pages(s
extern unsigned int vdso_enabled;

#define ARCH_DLINFO \
-do if (vdso_enabled) { \
+do if (vdso_enabled && sysctl_at_vsyscall) { \
    NEW_AUX_ENT(AT_SYSINFO, VDSO_ENTRY); \
    NEW_AUX_ENT(AT_SYSINFO_EHDR, VDSO_COMPAT_BASE); \
} while (0)
```

-mno-tls-direct-seg-refs"

Posted by [seyko2](#) on Sat, 16 Jun 2007 01:18:35 GMT

[View Forum Message](#) <> [Reply to Message](#)

```
#define ARCH_DLINFO          \
do {                          \
    NEW_AUX_ENT(AT_SYSINFO, VDSO_ENTRY);          \
    NEW_AUX_ENT(AT_SYSINFO_EHDR, VDSO_COMPAT_BASE); \
} while (0)
```

```
#define ARCH_DLINFO          \
do if (vdso_enabled) {      \
    NEW_AUX_ENT(AT_SYSINFO, VDSO_ENTRY);          \
    NEW_AUX_ENT(AT_SYSINFO_EHDR, VDSO_COMPAT_BASE); \
} while (0)
```

Posted by [dev](#) on Sat, 16 Jun 2007 17:59:47 GMT

[View Forum Message](#) <> [Reply to Message](#)

Posted by [seyko2](#) on Mon, 18 Jun 2007 13:52:22 GMT

[View Forum Message](#) <> [Reply to Message](#)

```
diff --git a/kernel/ve/vecalls.c b/kernel/ve/vecalls.c
index d1b55a8..5ade018 100644
--- a/kernel/ve/vecalls.c
+++ b/kernel/ve/vecalls.c
@@ -1193,7 +1193,7 @@ static int do_ve_iptables(struct ve_struct *ve, __u64 init_mask,
    init_mask &= ~VE_IP_IPTABLES6;
    init_mask &= ~VE_IP_FILTER6;
    init_mask &= ~VE_IP_MANGLE6;
-   init_mask &= ~VE_IP_IPTABLE_NAT;
+   init_mask &= ~VE_IP_IPTABLE_NAT_MOD;
    if ((init_mask & VE_IP_IPTABLES) == VE_IP_IPTABLES)
        init_mask |= VE_IP_IPTABLES6;
    if ((init_mask & VE_IP_FILTER) == VE_IP_FILTER)
```

Posted by [Andrey Mirkin](#) on Wed, 20 Jun 2007 13:39:02 GMT
[View Forum Message](#) <> [Reply to Message](#)

Posted by [seyko2](#) on Wed, 20 Jun 2007 13:49:03 GMT
[View Forum Message](#) <> [Reply to Message](#)

vdso)
