

[Full-disclosure] [USN-231-1] Linux kernel vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-12/msg01215.html>

- *From:* Martin Pitt <martin.pitt@xxxxxxxxxxxxxx>
 - *Date:* Thu, 22 Dec 2005 16:16:13 +0100
-

=====
Ubuntu Security Notice USN-231-1 December 22, 2005
linux-source-2.6.8.1/-2.6.10/-2.6.12 vulnerabilities
CVE-2005-3257, CVE-2005-3783, CVE-2005-3784, CVE-2005-3805,
CVE-2005-3806, CVE-2005-3808, CVE-2005-3848, CVE-2005-3857,
CVE-2005-3858
=====

A security issue affects the following Ubuntu releases:

- Ubuntu 4.10 (Warty Warthog)
- Ubuntu 5.04 (Hoary Hedgehog)
- Ubuntu 5.10 (Breezy Badger)

The following packages are affected:

- linux-image-2.6.10-6-386
- linux-image-2.6.10-6-686
- linux-image-2.6.10-6-686-smp
- linux-image-2.6.10-6-amd64-generic
- linux-image-2.6.10-6-amd64-k8
- linux-image-2.6.10-6-amd64-k8-smp
- linux-image-2.6.10-6-amd64-xeon
- linux-image-2.6.10-6-itanium
- linux-image-2.6.10-6-itanium-smp
- linux-image-2.6.10-6-k7
- linux-image-2.6.10-6-k7-smp
- linux-image-2.6.10-6-mckinley
- linux-image-2.6.10-6-mckinley-smp
- linux-image-2.6.10-6-power3
- linux-image-2.6.10-6-power3-smp
- linux-image-2.6.10-6-power4
- linux-image-2.6.10-6-power4-smp
- linux-image-2.6.10-6-powerpc
- linux-image-2.6.10-6-powerpc-smp
- linux-image-2.6.12-10-386
- linux-image-2.6.12-10-686
- linux-image-2.6.12-10-686-smp

[Full-disclosure] [USN-231-1] Linux kernel vulnerabilities

linux-image-2.6.12-10-amd64-generic
linux-image-2.6.12-10-amd64-k8
linux-image-2.6.12-10-amd64-k8-smp
linux-image-2.6.12-10-amd64-xeon
linux-image-2.6.12-10-iserics-smp
linux-image-2.6.12-10-k7
linux-image-2.6.12-10-k7-smp
linux-image-2.6.12-10-powerpc
linux-image-2.6.12-10-powerpc-smp
linux-image-2.6.12-10-powerpc64-smp
linux-image-2.6.8.1-6-386
linux-image-2.6.8.1-6-686
linux-image-2.6.8.1-6-686-smp
linux-image-2.6.8.1-6-amd64-generic
linux-image-2.6.8.1-6-amd64-k8
linux-image-2.6.8.1-6-amd64-k8-smp
linux-image-2.6.8.1-6-amd64-xeon
linux-image-2.6.8.1-6-k7
linux-image-2.6.8.1-6-k7-smp
linux-image-2.6.8.1-6-power3
linux-image-2.6.8.1-6-power3-smp
linux-image-2.6.8.1-6-power4
linux-image-2.6.8.1-6-power4-smp
linux-image-2.6.8.1-6-powerpc
linux-image-2.6.8.1-6-powerpc-smp
linux-patch-debian-2.6.8.1
linux-patch-ubuntu-2.6.10
linux-patch-ubuntu-2.6.12

The problem can be corrected by upgrading the affected package to version 2.6.8.1-16.26 (for Ubuntu 4.10), 2.6.10-34.9 (for Ubuntu 5.04), or 2.6.12-10.25 (for Ubuntu 5.10). After a standard system upgrade you need to reboot the computer to effect the necessary changes.

Details follow:

Rudolf Polzer reported an abuse of the 'loadkeys' command. By redefining one or more keys and tricking another user (like root) into logging in on a text console and typing something that involves the redefined keys, a local user could cause execution of arbitrary commands with the privileges of the target user. The updated kernel restricts the usage of 'loadkeys' to root. (CVE-2005-3257)

The ptrace() system call did not correctly check whether a process tried to attach to itself. A local attacker could exploit this to cause a kernel crash. (CVE-2005-3783)

A Denial of Service vulnerability was found in the handler that automatically cleans up and terminates child processes that are not correctly handled by their parent process ("auto-reaper"). The check

did not correctly handle processes which were currently traced by another process. A local attacker could exploit this to cause a kernel crash. (CVE-2005-3784)

A locking problem was discovered in the POSIX timer cleanup handling on process exit. A local attacker could exploit this to cause the machine to hang (Denial of Service). This flaw only affects multiprocessor (SMP) systems. (CVE-2005-3805)

A Denial of Service vulnerability was discovered in the IPv6 flowlabel handling code. By invoking `setsockopt(IPV6_FLOWLABEL_MGR)` in a special way, a local attacker could cause memory corruption which eventually led to a kernel crash. (CVE-2005-3806)

A memory leak was discovered in the VFS lease handling. These operations are commonly executed by the Samba server, which led to steady memory exhaustion. By repeatedly triggering the affected operations in quick succession, a local attacker could exploit this to drain all memory, which leads to a Denial of Service. (CVE-2005-3807)

An integer overflow was discovered in the `invalidate_inode_pages2_range()` function. By issuing 64-bit `mmap` calls on a 32 bit system, a local user could exploit this to crash the machine, thereby causing Denial of Service. This flaw does not affect the amd64 platform, and does only affect Ubuntu 5.10. (CVE-2005-3808)

Ollie Wild discovered a memory leak in the `icmp_push_reply()` function. By sending a large amount of specially crafted packets, a remote attacker could exploit this to drain all memory, which eventually leads to a Denial of Service. (CVE-2005-3848)

Chris Wriqth found a Denial of Service vulnerability in the `time_out_leases()` function. By allocating a large number of VFS file lock leases and having them timeout at the same time, a large number of 'printk' debugging statements was generated at the same time, which could exhaust kernel memory. (CVE-2005-3857)

Patrick McHardy discovered a memory leak in the `ip6_input_finish()` function. A remote attacker could exploit this by sending specially crafted IPv6 packets, which would eventually drain all available kernel memory, thus causing a Denial of Service. (CVE-2005-3858)

Updated packages for Ubuntu 4.10:

Source archives:

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-source-2.6.8.1_2.6.8.1-16.26.diff.gz
Size/MD5: 3170552 832cc0e756a1d6745fac1f1192164051

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-source-2.6.8.1_2.6.8.1-16.26.dsc
Size/MD5: 2621 d80a34d63f68d57cf9b41e3a62d8a5fd

[Full-disclosure] [USN-231-1] Linux kernel vulnerabilities

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-source-2.6.8.1_2.6.8.1.orig.tar.gz
Size/MD5: 44728688 79730a3ad4773ba65fab65515369df84

Architecture independent packages:

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-doc-2.6.8.1_2.6.8.1-16.26_all.deb
Size/MD5: 6163566 a2cead0ca74ab15480b77d971345da04

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-patch-debian-2.6.8.1_2.6.8.1-16.26_all.deb
Size/MD5: 1525504 eda4efc1e49ae2fc3d125a9e55c0e8a2

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-source-2.6.8.1_2.6.8.1-16.26_all.deb
Size/MD5: 36727926 68646a3965e9a68ee380e66528653d1a

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-tree-2.6.8.1_2.6.8.1-16.26_all.deb
Size/MD5: 310734 b1af150de1f688ec90bd8a63666673a9

amd64 architecture (Athlon64, Opteron, EM64T Xeon)

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-6-amd64-generic_2.6.8.1-16.26_all.deb
Size/MD5: 250446 c2825f1ad32acd2e3e1e7f209518d1f0

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-6-amd64-k8-smp_2.6.8.1-16.26_all.deb
Size/MD5: 245676 5f41d408017acfe5ef2472366df67f0e

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-6-amd64-k8_2.6.8.1-16.26_all.deb
Size/MD5: 249428 4800655fdd579a236872b6209c619d8f

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-6-amd64-xeon_2.6.8.1-16.26_all.deb
Size/MD5: 244160 7a6b0f5a27f5e598468e35ce8f9d9b44

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-6_2.6.8.1-16.26_amd64.deb
Size/MD5: 3181900 efe94f286a7ad2acfc11502e2758843e

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-6-amd64-generic_2.6.8.1-16.26_all.deb
Size/MD5: 14355574 8bd6fa79b06b53e21d5386d8689f5f7e

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-6-amd64-k8-smp_2.6.8.1-16.26_all.deb
Size/MD5: 14834294 ff7d860ed947f0055e0cc3e33c49c1f5

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-6-amd64-k8_2.6.8.1-16.26_all.deb
Size/MD5: 14867554 cc996f71eb6fb830be6a88305e8405cf

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-6-amd64-xeon_2.6.8.1-16.26_all.deb
Size/MD5: 14689444 068a59e07779c886a8f39495219c2e59

i386 architecture (x86 compatible Intel/AMD)

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-6-386_2.6.8.1-16.26_i386.deb
Size/MD5: 279392 31a606be538eb5b4a0039f9245e50a0e

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-6-686-smp_2.6.8.1-16.26_i386.deb
Size/MD5: 274480 8cb3539e6ccf850f39a12fca99c5824f

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-6-686_2.6.8.1-16.26_i386.deb
Size/MD5: 277424 f243af08bc7b971c00c7f1911957cc0b

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-6-k7-smp_2.6.8.1-16.26_i386.deb
Size/MD5: 274668 676b1cdbb07daaf1e59daf4379f90d41

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-6-k7_2.6.8.1-16.26_i386.deb
Size/MD5: 277316 2e4b212e8851b8ebecb6e11fc4e95c4

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-6_2.6.8.1-16.26_i386.deb
Size/MD5: 3222690 c0a49e48f2acbcfa8158e1d3508edf4d

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-6-386_2.6.8.1-16.26_i386.deb
Size/MD5: 15499122 c057a0f020e65f820616480dec86efd7

[Full-disclosure] [USN-231-1] Linux kernel vulnerabilities

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-6-686-smp_2.6.8.1-16.26
Size/MD5: 16350082 077cd7705843e9735b97523fc68d848a
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-6-686_2.6.8.1-16.26_i386
Size/MD5: 16522126 c5107134a7df85767ba34f7ea2aa8f3c
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-6-k7-smp_2.6.8.1-16.26_i
Size/MD5: 16451508 437e3bdc941350ffe378737124b5b1
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-6-k7_2.6.8.1-16.26_i386.d
Size/MD5: 16577002 b51a395a23cf6cc4e2db48e21e9059a4

powerpc architecture (Apple Macintosh G3/G4/G5)

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-6-power3-smp_2.6.8.1-1
Size/MD5: 215406 31367d21f92a1652a8edbd0857930a6d
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-6-power3_2.6.8.1-16.26
Size/MD5: 216288 ae1eb9335c762606e4d85a4cd8bfdceb
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-6-power4-smp_2.6.8.1-1
Size/MD5: 215300 840f755ebafa0a4f1aa735767288d113
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-6-power4_2.6.8.1-16.26
Size/MD5: 216050 aa22681d63977507c4968c9d12bacbf7
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-6-powerpc-smp_2.6.8.1-1
Size/MD5: 215766 0f42c778baae6668cd7f0892aca80dc3
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-6-powerpc_2.6.8.1-16.26
Size/MD5: 217834 d71d028a66ef8d08540164b5f5d0a07e
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-6_2.6.8.1-16.26_powerpc
Size/MD5: 3299816 2c8ce356254d6666bd09d1ddc416aa96
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-6-power3-smp_2.6.8.1-16
Size/MD5: 16376792 ee18a809e85d8ec02f0b876edbc7b7aa
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-6-power3_2.6.8.1-16.26_p
Size/MD5: 15941840 17d5cee523dad9e01ebf73e448d29ffc
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-6-power4-smp_2.6.8.1-16
Size/MD5: 16362160 96ac56ba61e5e512b94fb94d80296013
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-6-power4_2.6.8.1-16.26_p
Size/MD5: 15934294 91e46887699a93fef26669485768a1fa
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-6-powerpc-smp_2.6.8.1-1
Size/MD5: 16296020 e27f3e627f2261fc2ed2cd2d5f75c835
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-6-powerpc_2.6.8.1-16.26
Size/MD5: 15977246 cde71c6f5f13350170d3dc35c2acbd71

Updated packages for Ubuntu 5.04:

Source archives:

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-source-2.6.10_2.6.10-34.9.diff.gz
Size/MD5: 6106913 4ab709e955455a8462ed14b6bf23765c
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-source-2.6.10_2.6.10-34.9.dsc
Size/MD5: 3145 d0ec696544bf43603e3fb7d4bee59aae
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-source-2.6.10_2.6.10.orig.tar.gz
Size/MD5: 46244465 063a64fc0efd9c9901cf07effef1b747

Architecture independent packages:

[Full-disclosure] [USN-231-1] Linux kernel vulnerabilities

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-doc-2.6.10_2.6.10-34.9_all.deb
Size/MD5: 6786114 b9ca3648c990ac6a818bf9d23901e5b8
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-source-2.6.10_2.6.10-34.9_all.deb
Size/MD5: 37514576 a3ca3007277f1d6087eb9d5c04d5339f
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-tree-2.6.10_2.6.10-34.9_all.deb
Size/MD5: 505088 5fea08f2c855390168beaff3d3a85aef

amd64 architecture (Athlon64, Opteron, EM64T Xeon)

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/acpi-modules-2.6.10-6-amd64-generic-di_2.6.10-34.9_all.deb
Size/MD5: 20824 4cd45992f8d434ab12ba02ac1ff5287d
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/cdrom-core-modules-2.6.10-6-amd64-generic-di_2.6.10-34.9_all.deb
Size/MD5: 47392 db52b9fd7e86d5516e087c769aec2ba1
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/ext3-modules-2.6.10-6-amd64-generic-di_2.6.10-34.9_all.deb
Size/MD5: 88898 7571117b0d474659d22be36d52c4e90b
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/fat-modules-2.6.10-6-amd64-generic-di_2.6.10-34.9_all.deb
Size/MD5: 30020 21b0e4c54e81371bc0650f0880662856
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/fb-modules-2.6.10-6-amd64-generic-di_2.6.10-34.9_all.deb
Size/MD5: 41242 bc305f667fd84710aa02cb8b975f3f9f
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/firewire-core-modules-2.6.10-6-amd64-generic-di_2.6.10-34.9_all.deb
Size/MD5: 73596 7688e093de1a4ced4e15f7edd9a60d7a
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/firmware-modules-2.6.10-6-amd64-generic-di_2.6.10-34.9_all.deb
Size/MD5: 5736 37a5030470f6932bde183af4f79b115a
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/floppy-modules-2.6.10-6-amd64-generic-di_2.6.10-34.9_all.deb
Size/MD5: 34852 84eb464811f314db0ba9ab2601b90dbd
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/ide-core-modules-2.6.10-6-amd64-generic-di_2.6.10-34.9_all.deb
Size/MD5: 55184 24a20b6a3fd1de72562582ea2cd55f5e
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/ide-modules-2.6.10-6-amd64-generic-di_2.6.10-34.9_all.deb
Size/MD5: 112986 6baef547b8cb4065fa636fff6813d481
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/input-modules-2.6.10-6-amd64-generic-di_2.6.10-34.9_all.deb
Size/MD5: 40808 81a10edd2bc8cfa18469190e556222e8
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/ipv6-modules-2.6.10-6-amd64-generic-di_2.6.10-34.9_all.deb
Size/MD5: 115724 d4345cb047f346cb99322e9ad0b73b12
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/irda-modules-2.6.10-6-amd64-generic-di_2.6.10-34.9_all.deb
Size/MD5: 174640 21a69880d0757086530e0889d39e6995
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/jfs-modules-2.6.10-6-amd64-generic-di_2.6.10-34.9_all.deb
Size/MD5: 82594 d3a263147fcae21c67b21c5b75968ade
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/kernel-image-2.6.10-6-amd64-generic-di_2.6.10-34.9_all.deb
Size/MD5: 1467028 dcca60d1954caaed9747fecacdd93af3
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-headers-2.6.10-6-amd64-generic_2.6.10-34.9_all.deb
Size/MD5: 286854 18ef5a2c4203c08207258e75443d413d
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-headers-2.6.10-6-amd64-k8-smp_2.6.10-34.9_all.deb
Size/MD5: 283700 9a3152f95df24f5838fb493f5c858768
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-headers-2.6.10-6-amd64-k8_2.6.10-34.9_all.deb
Size/MD5: 285652 a5e893bd70c1cf20b2f8e4db7b02e9ed
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-headers-2.6.10-6-amd64-xeon_2.6.10-34.9_all.deb
Size/MD5: 281160 0eeb78731437357459b67ff41b258d3f
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-headers-2.6.10-6_2.6.10-34.9_amd64.deb
Size/MD5: 6138076 971e8c65aa1d9ef9706d765c2ff25428
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-image-2.6.10-6-amd64-generic_2.6.10-34.9_all.deb
Size/MD5: 14577226 132c0d8cb07cce4b39a17d8224f9b214

[Full-disclosure] [USN-231-1] Linux kernel vulnerabilities

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-image-2.6.10-6-amd64-k8-smp_2.6.10-34.9_amd64.deb
Size/MD5: 15121616 fdd5425104067c12d4450b892335830e

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-image-2.6.10-6-amd64-k8_2.6.10-34.9_amd64.deb
Size/MD5: 15089954 eff3971f7ca98fe85c76e58ad9383287

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-image-2.6.10-6-amd64-xeon_2.6.10-34.9_amd64.deb
Size/MD5: 14960698 11144e3d069cb021b30436a0b6e1343f

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-patch-ubuntu-2.6.10_2.6.10-34.9_amd64.deb
Size/MD5: 1363088 098539c9c1323acee8a8376d27d43082

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/loop-modules-2.6.10-6-amd64-generic-di_2.6.10-34.9_amd64.deb
Size/MD5: 14228 a5c7e990e2bd73d5ffa0bea864bfb2cc

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/md-modules-2.6.10-6-amd64-generic-di_2.6.10-34.9_amd64.deb
Size/MD5: 178486 6bf3b6eb9fcb296fd399314fd3ab01e0

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/nfs-modules-2.6.10-6-amd64-generic-di_2.6.10-34.9_amd64.deb
Size/MD5: 174852 63c4f98092b8295a8f78f9c5e46fcc46

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/nic-extra-modules-2.6.10-6-amd64-generic-di_2.6.10-34.9_amd64.deb
Size/MD5: 731132 d70252df3aa69e982099bac2997f0b52

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/nic-firmware-2.6.10-6-amd64-generic-di_2.6.10-34.9_amd64.deb
Size/MD5: 780918 6974a907c34f25c99ee592cd792d9b23

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/nic-modules-2.6.10-6-amd64-generic-di_2.6.10-34.9_amd64.deb
Size/MD5: 150020 37a9d821e9f0ca67987f5eeafe90d3e9

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/nic-pcmcia-modules-2.6.10-6-amd64-generic-di_2.6.10-34.9_amd64.deb
Size/MD5: 168122 62cd7e3c16281c74013f0035fc523aac

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/nic-shared-modules-2.6.10-6-amd64-generic-di_2.6.10-34.9_amd64.deb
Size/MD5: 9554 2d36e8303bbf31cff1970c0b808a1e97

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/nic-usb-modules-2.6.10-6-amd64-generic-di_2.6.10-34.9_amd64.deb
Size/MD5: 94856 ce272989496145c8c466d8ea7d7fb209

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/ntfs-modules-2.6.10-6-amd64-generic-di_2.6.10-34.9_amd64.deb
Size/MD5: 45730 525cad65ab4b9945302c0de920ffdfc4

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/parport-modules-2.6.10-6-amd64-generic-di_2.6.10-34.9_amd64.deb
Size/MD5: 33156 8057008f1a18f79c043e1b3b3e511508

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/pcmcia-modules-2.6.10-6-amd64-generic-di_2.6.10-34.9_amd64.deb
Size/MD5: 55280 64c0a4496e0c9f63287abb051df482b9

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/pcmcia-storage-modules-2.6.10-6-amd64-generic-di_2.6.10-34.9_amd64.deb
Size/MD5: 4662 cc6e49f1ef31a094d358fdd0b54068a8

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/plip-modules-2.6.10-6-amd64-generic-di_2.6.10-34.9_amd64.deb
Size/MD5: 7840 534f69488f84a855ed44e2257bcdbe11

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/ppp-modules-2.6.10-6-amd64-generic-di_2.6.10-34.9_amd64.deb
Size/MD5: 53796 7a591b707bb66b847f32ff1f99f586fb

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/reiserfs-modules-2.6.10-6-amd64-generic-di_2.6.10-34.9_amd64.deb
Size/MD5: 111112 5894f5dcc627e706f3b46cee814fe82c

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/rtc-modules-2.6.10-6-amd64-generic-di_2.6.10-34.9_amd64.deb
Size/MD5: 10160 ee7a9f07d183603c31cdc00b52ef0d07

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/sata-modules-2.6.10-6-amd64-generic-di_2.6.10-34.9_amd64.deb
Size/MD5: 60460 034ac891de70103fc676ea8453154b16

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/scsi-common-modules-2.6.10-6-amd64-generic-di_2.6.10-34.9_amd64.deb
Size/MD5: 208570 f65c80ab64e461736a5a3cc44a77fd07

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/scsi-core-modules-2.6.10-6-amd64-generic-di_2.6.10-34.9_amd64.deb
Size/MD5: 69258 cf4dc68bbc5d42d2a09d3bd38497f00d

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/scsi-extra-modules-2.6.10-6-amd64-generic-di_2.6.10-34.9_amd64.deb
Size/MD5: 394754 b0bf8e097102ac7d69d8220be8abc2e8

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/scsi-modules-2.6.10-6-amd64-generic-di_2.6.10-34.9_amd64.deb

[Full-disclosure] [USN-231-1] Linux kernel vulnerabilities

Size/MD5: 310708 3cd8dfc15e0b86698845ce04c2fda6fd
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-headers-2.6.10-6-686_2.6.10-34.9_i386.deb
Size/MD5: 313226 73a5fb5f5b3beb9c3bbbf5e775b5902
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-headers-2.6.10-6-k7-smp_2.6.10-34.9_i386.deb
Size/MD5: 311036 e68ab83e930fff7287e7b7679be31cab
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-headers-2.6.10-6-k7_2.6.10-34.9_i386.deb
Size/MD5: 312970 9f2307bea370e147ec28a3dadb045da9
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-headers-2.6.10-6_2.6.10-34.9_i386.deb
Size/MD5: 6134562 2291c5493bd96bf3e4861618c78adbcd
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-image-2.6.10-6-386_2.6.10-34.9_i386.deb
Size/MD5: 15613984 3ac32df50e98bb1dba331127af31bdf9
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-image-2.6.10-6-686-smp_2.6.10-34.9_i386.deb
Size/MD5: 16189224 6fb46eaf0ae88cf0913a5ee9e1a0b1db
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-image-2.6.10-6-686_2.6.10-34.9_i386.deb
Size/MD5: 16606866 3d5deefb44f6d281f417030e8b96a0d4
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-image-2.6.10-6-k7-smp_2.6.10-34.9_i386.deb
Size/MD5: 16300716 d88aa98c7aa1606d15f7fff7d19a0634
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-image-2.6.10-6-k7_2.6.10-34.9_i386.deb
Size/MD5: 16672004 da91e8ebf85d34db7a7a688f768aa206
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-patch-ubuntu-2.6.10_2.6.10-34.9_i386.deb
Size/MD5: 1364358 f955ba8b0d2d313cd99454f89a35a840
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/loop-modules-2.6.10-6-386-di_2.6.10-34.9_i386.deb
Size/MD5: 14078 72df7aa7675563386a8be118c583c5a7
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/md-modules-2.6.10-6-386-di_2.6.10-34.9_i386.deb
Size/MD5: 183162 027cce78046f76ffb904433f9408b81c
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/nfs-modules-2.6.10-6-386-di_2.6.10-34.9_i386.deb
Size/MD5: 172742 265dc115ccda3c41db6c20b709e766bc
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/nic-extra-modules-2.6.10-6-386-di_2.6.10-34.9_i386.deb
Size/MD5: 967836 3b2532d6e6a0e5d029b508d934060ca0
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/nic-firmware-2.6.10-6-386-di_2.6.10-34.9_i386.deb
Size/MD5: 780720 2666c3218f5778dc8a0df50abe6ce0d9
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/nic-modules-2.6.10-6-386-di_2.6.10-34.9_i386.deb
Size/MD5: 140652 6ef2cc8a219e16097062f608ce0487e1
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/nic-pcmcia-modules-2.6.10-6-386-di_2.6.10-34.9_i386.deb
Size/MD5: 167956 5c5f177a0d2504351cddf851c03c13c5
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/nic-shared-modules-2.6.10-6-386-di_2.6.10-34.9_i386.deb
Size/MD5: 9346 67c477552c37417992d9502f4a0decb7
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/nic-usb-modules-2.6.10-6-386-di_2.6.10-34.9_i386.deb
Size/MD5: 89324 34289867bffeef0cf13fc86020f33a25
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/nfs-modules-2.6.10-6-386-di_2.6.10-34.9_i386.deb
Size/MD5: 48134 b95adb553852c7fccb4483778e54bbfa
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/parport-modules-2.6.10-6-386-di_2.6.10-34.9_i386.deb
Size/MD5: 30876 0f896585830110f82b67752c9d23b113
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/pcmcia-modules-2.6.10-6-386-di_2.6.10-34.9_i386.deb
Size/MD5: 65890 1048a67e1bc9ac646697dfc859ce0241
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/pcmcia-storage-modules-2.6.10-6-386-di_2.6.10-34.9_i386.deb
Size/MD5: 4506 42396bfae1cd96959153f871326f4f98
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/plip-modules-2.6.10-6-386-di_2.6.10-34.9_i386.deb
Size/MD5: 7754 21c6e394830dff9804fe4bb3069bcef5
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/ppp-modules-2.6.10-6-386-di_2.6.10-34.9_i386.deb
Size/MD5: 50776 2d8c712690246434194a7695b9c2594e

[Full-disclosure] [USN-231-1] Linux kernel vulnerabilities

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/reiserfs-modules-2.6.10-6-386-di_2.6.10-34.9
Size/MD5: 111586 f8c63e68258d959b0cdc7a6bdb38e0c5

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/rtc-modules-2.6.10-6-386-di_2.6.10-34.9_i386
Size/MD5: 9892 fff1d44c3afe5483763b0de15c3be859

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/sata-modules-2.6.10-6-386-di_2.6.10-34.9_i386
Size/MD5: 57162 3c75eae233f3d237b14df40c8c6c9891

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/scsi-common-modules-2.6.10-6-386-di_2.6.10-34.9_i386
Size/MD5: 241936 fea5caa83d99ec03fa066a2f749f0dc1

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/scsi-core-modules-2.6.10-6-386-di_2.6.10-34.9_i386
Size/MD5: 66236 00458daa87e419708154fd6ac381a908

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/scsi-extra-modules-2.6.10-6-386-di_2.6.10-34.9_i386
Size/MD5: 436536 1aef4e9dec409ce72a231c4511b27140

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/scsi-modules-2.6.10-6-386-di_2.6.10-34.9_i386
Size/MD5: 485680 5c6df01891466e59f1e5fa1838c72679

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/serial-modules-2.6.10-6-386-di_2.6.10-34.9_i386
Size/MD5: 11472 c5d7dc5acb91ad128bbf3179304d0cc8

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/socket-modules-2.6.10-6-386-di_2.6.10-34.9_i386
Size/MD5: 21246 ce695efe91904d2e8780c838ac34405c

http://security.ubuntu.com/ubuntu/pool/universe/l/linux-source-2.6.10/ufs-modules-2.6.10-6-386-di_2.6.10-34.9_i386
Size/MD5: 29530 69bb84e0d25130cadd0edee6c6ff03b4

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/usb-modules-2.6.10-6-386-di_2.6.10-34.9_i386
Size/MD5: 106268 497386cabff8b1e7f816d35a502a698c

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/usb-storage-modules-2.6.10-6-386-di_2.6.10-34.9_i386
Size/MD5: 33822 4f694243ad5741b7f149bba57d9e5af7

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/xfstools-modules-2.6.10-6-386-di_2.6.10-34.9_i386
Size/MD5: 261340 3ed237bb00e4edede1cc4c530ebcca6a

powerpc architecture (Apple Macintosh G3/G4/G5)

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/affs-modules-2.6.10-6-power3-di_2.6.10-34.9
Size/MD5: 24052 dd5123228e1296229f6ae5bcd90274bc

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/affs-modules-2.6.10-6-power4-di_2.6.10-34.9
Size/MD5: 24052 9ae1156032597e08a95ce5ddc2ed7c63

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/affs-modules-2.6.10-6-powerpc-di_2.6.10-34.9
Size/MD5: 24038 6c746dc8b8e0365f6dddee5d558faf09

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/cdrom-core-modules-2.6.10-6-power3-di_2.6.10-34.9
Size/MD5: 58272 23825b63c98e3f1126abb4c13aa5d40c

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/cdrom-core-modules-2.6.10-6-power4-di_2.6.10-34.9
Size/MD5: 58278 1742c098aa32508297c8aa49e20c99fd

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/cdrom-core-modules-2.6.10-6-powerpc-di_2.6.10-34.9
Size/MD5: 58256 f501150d3760b8103ff73fbf9738e251

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/ext2-modules-2.6.10-6-power3-di_2.6.10-34.9
Size/MD5: 30284 870763b979da02d74043947e238e4166

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/ext2-modules-2.6.10-6-power4-di_2.6.10-34.9
Size/MD5: 30280 9b050ba2eb98a101c88f73fc93b0821b

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/ext2-modules-2.6.10-6-powerpc-di_2.6.10-34.9
Size/MD5: 30266 99f22e3d3280351a4e015916256d1617

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/ext3-modules-2.6.10-6-power3-di_2.6.10-34.9
Size/MD5: 109248 552aa39534ed4f71d0c0a34aa66047e4

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/ext3-modules-2.6.10-6-power4-di_2.6.10-34.9
Size/MD5: 109246 511a988baad89dd12388632545088a14

[Full-disclosure] [USN-231-1] Linux kernel vulnerabilities

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/ext3-modules-2.6.10-6-powerpc-di_2.6.10-34.9
Size/MD5: 109220 dfb264ed5a710951637ee7bd75933321

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/fat-modules-2.6.10-6-power3-di_2.6.10-34.9
Size/MD5: 35386 a991857d43e86b17c61cf65c27d114a1

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.12/ppp-modules-2.6.12-10-powerpc-di_2.6.12-10
Size/MD5: 63072 2bb8eb763bcc7b277375b17dfa83ec7e

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.12/ppp-modules-2.6.12-10-powerpc64-smp-di_2.6.12-10
Size/MD5: 75992 ef969b2a8f51c64f0996c8de6786affc

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.12/reiserfs-modules-2.6.12-10-powerpc-di_2.6.12-10
Size/MD5: 128628 039558a693c99fabb88878fad8037146

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.12/reiserfs-modules-2.6.12-10-powerpc64-smp-di_2.6.12-10
Size/MD5: 164352 971f1f781022575cc0c8f821dcf34075

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.12/sata-modules-2.6.12-10-powerpc-di_2.6.12-10
Size/MD5: 77424 415ceb336e4647489a8a58e7ab3c9da0

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.12/sata-modules-2.6.12-10-powerpc64-smp-di_2.6.12-10
Size/MD5: 98172 3711b5b68e89a953cf1825519b0181b7

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.12/scsi-core-modules-2.6.12-10-powerpc-di_2.6.12-10
Size/MD5: 85244 11999af2636c69db05e1486daaf50f60

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.12/scsi-core-modules-2.6.12-10-powerpc64-smp-di_2.6.12-10
Size/MD5: 92318 7d276803baf7fdf423efd10346c17d39

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.12/scsi-modules-2.6.12-10-powerpc-di_2.6.12-10
Size/MD5: 1537736 3cf2ba8dcba03eb117f8eab95354989

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.12/scsi-modules-2.6.12-10-powerpc64-smp-di_2.6.12-10
Size/MD5: 1755504 a1dc1b25ccfeb128e6c7fb10c9ea7b0a

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.12/serial-modules-2.6.12-10-powerpc-di_2.6.12-10
Size/MD5: 65300 ddf32661c0d5e1fe5beead5353e0b2e9