

[Full-disclosure] [USN-263-1] Linux kernel vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2006-03/msg00704.html>

- *From:* Martin Pitt <martin.pitt@xxxxxxxxxxxxxx>
 - *Date:* Mon, 13 Mar 2006 11:32:35 +0100
-

=====
Ubuntu Security Notice USN-263-1 March 13, 2006
linux-source-2.6.8.1/-2.6.10/-2.6.12 vulnerabilities
CVE-2005-3359, CVE-2006-0457, CVE-2006-0554, CVE-2006-0555,
CVE-2006-0741, CVE-2006-0742
=====

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
- linux-image-2.6.12-10-amd64-generic

[Full-disclosure] [USN-263-1] Linux kernel vulnerabilities

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-itanium
linux-image-2.6.12-10-itanium-smp
linux-image-2.6.12-10-k7
linux-image-2.6.12-10-k7-smp
linux-image-2.6.12-10-mckinley
linux-image-2.6.12-10-mckinley-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 2.6.8.1-16.28 (for Ubuntu 4.10), 2.6.10-34.12 (for Ubuntu 5.04), or 2.6.12-10.30 (for Ubuntu 5.10). After a standard system upgrade you need to reboot your machine to effect the necessary changes.

Details follow:

A flaw was found in the module reference counting for loadable protocol modules of netfilter. By performing particular socket operations, a local attacker could exploit this to crash the kernel. This flaw only affects Ubuntu 5.10. (CVE-2005-3359)

David Howells noticed a race condition in the `add_key()`, `request_key()` and `keyctl()` functions. By modifying the length of string arguments after the kernel determined their length, but before the kernel copied them into kernel memory, a local attacker could either crash the kernel or read random parts of kernel memory (which could potentially contain sensitive data). (CVE-2006-0457)

An information disclosure vulnerability was discovered in the `truncate()` function for the XFS file system. Under certain conditions, this function could expose random unallocated blocks. A local user could potentially exploit this to recover sensitive data from previously deleted files. (CVE-2006-0554)

A local Denial of Service vulnerability was found in the NFS client module. By opening a file on an NFS share with `O_DIRECT` and performing some special operations on it, a local attacker could trigger a kernel crash. (CVE-2006-0555)

The ELF binary loader did not sufficiently verify some addresses in the ELF headers. By attempting to execute a specially crafted program, a local attacker could exploit this to trigger a recursive loop of kernel errors, which finally ended in a kernel crash. This only affects the amd64 architecture on Intel processors (EMT64). (CVE-2006-0741)

The `die_if_kernel()` function was incorrectly declared as "does never return" on the ia64 platform. A local attacker could exploit this to crash the kernel. Please note that ia64 is not an officially supported platform. (CVE-2006-0742)

Oleg Nesterov discovered a race condition in the signal handling. On multiprocessor (SMP) machines, a local attacker could exploit this to create many unkillable processes, which could eventually lead to a Denial of Service.

A memory leak was discovered in the handling of files which were opened with the `O_DIRECT` flag. By repeatedly opening files in a special way, a local attacker could eventually drain all available kernel memory and render the machine unusable. This flaw only affects Ubuntu 4.10.

(<http://linux.bkbits.net:8080/linux-2.6/cset%404182a613oVsK0-8eCWpyYFrUf8rhLA>)

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_2.6.8.1-16.28.diff.gz
Size/MD5: 3177048 738c05f96f03c3d95each978ed566d5a

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-source-2.6.8.1_2.6.8.1-16.28.dsc
Size/MD5: 1985 4edc606f4f8d70ff073893a5f8a550f3

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_2.6.8.1-16.28_all.deb

[Full-disclosure] [USN-263-1] Linux kernel vulnerabilities

Size/MD5: 6160554 76ffc0999455f0459a93df39840c4cb5

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-patch-debian-2.6.8.1_2.6.8.1-16.28_all.deb

Size/MD5: 1524520 9eda7aac66eda90f7b35db9b9867ef5f

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-source-2.6.8.1_2.6.8.1-16.28_all.deb

Size/MD5: 36732410 6b727ab5c03ac7609a6c624d28a5934a

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-tree-2.6.8.1_2.6.8.1-16.28_all.deb

Size/MD5: 311150 b3f9eeaf828bd1df73e25d9d09231bd3

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_2.6.8.1-16.28_amd64.deb

Size/MD5: 250972 1af7366af1995c66ec453d3cc2b2cd59

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-6-amd64-k8-smp_2.6.8.1-16.28_amd64.deb

Size/MD5: 245866 7a82395367a439c1f33a3e1066879414

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-6-amd64-k8_2.6.8.1-16.28_amd64.deb

Size/MD5: 249922 0a444eef0e9a47c81e22975fb386125

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-6-amd64-xeon_2.6.8.1-16.28_amd64.deb

Size/MD5: 244448 035204a962da5da1cabeda5e52786ef2

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-6_2.6.8.1-16.28_amd64.deb

Size/MD5: 3182352 86bcb90233b742316c0dca5929eed206

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-6-amd64-generic_2.6.8.1-16.28_amd64.deb

Size/MD5: 14356806 86e6309f1af17fa962b400234d49b760

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-6-amd64-k8-smp_2.6.8.1-16.28_amd64.deb

Size/MD5: 14835804 8c4401736f3916fd9b7a6ebdd3362e5b

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-6-amd64-k8_2.6.8.1-16.28_amd64.deb

Size/MD5: 14870476 1000b35f31ed4cc7d200fa88c14bbb88

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-6-amd64-xeon_2.6.8.1-16.28_amd64.deb

Size/MD5: 14690812 9958220ca6752354baa9493c6987b6af

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_2.6.8.1-16.28_i386.deb

Size/MD5: 279528 fac4e3be0c66dfb35d54ccb92258ccc9

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-6-686-smp_2.6.8.1-16.28_i386.deb

Size/MD5: 274856 4d7e373a764be8276c96ae6befb1c8cc

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-6-686_2.6.8.1-16.28_i386.deb

Size/MD5: 277474 68fabbaef877b486d0fd97790c199bb9

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-6-k7-smp_2.6.8.1-16.28_i386.deb

Size/MD5: 275020 01536871ecec29e74f2c85b23e3a4dfb

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-6-k7_2.6.8.1-16.28_i386.deb

Size/MD5: 277846 7e00ba42f31a83ba3f4aaefcddaebbf

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-6_2.6.8.1-16.28_i386.deb

Size/MD5: 3223066 cb4bfb6bcd13e1ee0e0713e8e82ca6cb

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-6-386_2.6.8.1-16.28_i386.deb

Size/MD5: 15498824 91ccc16eaf0db7732d0867a3b045255

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-6-686-smp_2.6.8.1-16.28_i386.deb

Size/MD5: 16352576 7e5d44cf5af7ed43bf2c902240da7c4f

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-6-686_2.6.8.1-16.28_i386.deb

Size/MD5: 16522252 7b9973aebd71a4e2f531c4c327dad9f7

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-6-k7-smp_2.6.8.1-16.28_i386.deb

Size/MD5: 16453628 888ad24d9aed22d4c2592c142cf5bb27

[Full-disclosure] [USN-263-1] Linux kernel vulnerabilities

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-6-k7_2.6.8.1-16.28_i386.d
Size/MD5: 16578592 7724dfc08d83e77c132c3405e20e15f1

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_2.6.8.1-16.28_i386.d
Size/MD5: 215932 a26d246c13cb9d7a3dc5988842686b59

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-6-power3_2.6.8.1-16.28_i386.d
Size/MD5: 216784 144707814d0ae7b45b897fd2b9791d81

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-6-power4-smp_2.6.8.1-16.28_i386.d
Size/MD5: 215592 730a4a134e1f84e23de8c824dfaf2c6c

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-6-power4_2.6.8.1-16.28_i386.d
Size/MD5: 216806 742faf58e5f0216ffa895318076411e1

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-6-powerpc-smp_2.6.8.1-16.28_i386.d
Size/MD5: 216306 0091c95dd463e473ce1dd9fc879b0b26

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-6-powerpc_2.6.8.1-16.28_i386.d
Size/MD5: 218322 bd9008fc7dda3e11194cfa41f95f656d

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-6_2.6.8.1-16.28_powerpc_i386.d
Size/MD5: 3300016 381099fe2fd65823f7a600798a0d04f9

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-6-power3-smp_2.6.8.1-16.28_i386.d
Size/MD5: 16377582 511942f4cae4b198ef4eb18a4f692c17

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-6-power3_2.6.8.1-16.28_i386.d
Size/MD5: 15943062 8e674424034bcea4db1fbc5cdcdd21be

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-6-power4-smp_2.6.8.1-16.28_i386.d
Size/MD5: 16361818 e4b2f0fe2b2c3b1af4410d4aa9482adb

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-6-power4_2.6.8.1-16.28_i386.d
Size/MD5: 15935226 9783ea2b9f1f9683b865c8b9886f9aa6

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-6-powerpc-smp_2.6.8.1-16.28_i386.d
Size/MD5: 16295862 f1e04dba3bc7f5f06a0e4e49a69b2615

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-6-powerpc_2.6.8.1-16.28_i386.d
Size/MD5: 15978332 80c0eb4c5714014c51c742b04f7b9071

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_2.6.10-34.12.diff.gz
Size/MD5: 7427315 72e4e034878080e863686f5101aa8b19

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-source-2.6.10_2.6.10-34.12.dsc
Size/MD5: 2511 8bcce24c6422230960e82ca26087cfc4

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:

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-doc-2.6.10_2.6.10-34.12_all.deb
Size/MD5: 6780254 881ddf846fdb04becec24f6a44b6d39d

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-source-2.6.10_2.6.10-34.12_all.deb
Size/MD5: 37519502 4756e568160853766ff8d52725f1c9a1

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-tree-2.6.10_2.6.10-34.12_all.deb
Size/MD5: 505522 00ea925943c0e1f6b0ac861050998b8c

[Full-disclosure] [USN-263-1] Linux kernel vulnerabilities

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_2.6.10-34.12_i386.deb
Size/MD5: 20834 0c273229a33cc1ba40e7d75fd829db19

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/cdrom-core-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_i386.deb
Size/MD5: 47400 6794040f3a5ef0265e0d1ff2ac22a299

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/ext3-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_i386.deb
Size/MD5: 88898 60dc8192d66f9e4f9b03e5c2b53f66cc

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/fat-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_i386.deb
Size/MD5: 30024 9642b4bba83f038568f3865d707a4be4

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/fb-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_i386.deb
Size/MD5: 41246 1df552bf4fca7ea844b9759712cc586a

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/firewire-core-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_i386.deb
Size/MD5: 73604 ae712927df5a96a16bd502a736f73989

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/firmware-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_i386.deb
Size/MD5: 5744 3bd2f3d9318161497df6f5c8bfd957a7

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/floppy-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_i386.deb
Size/MD5: 34856 e7d5d8a3e021b295768ca7f73f52abcf

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/ide-core-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_i386.deb
Size/MD5: 55186 fb4a0661af0a190c5f23cadb0206081a

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/ide-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_i386.deb
Size/MD5: 112948 2d9e4b391555f60904041be5724ca489

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/input-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_i386.deb
Size/MD5: 40826 738b526f33a529b5b226350ba2c5a0ac

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/ipv6-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_i386.deb
Size/MD5: 115726 f1d30259e5038e7a7312231ffb78e91f

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/irda-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_i386.deb
Size/MD5: 174638 cea12eb3752058beff47c732c044a797

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/jfs-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_i386.deb
Size/MD5: 82594 4ba09c52af79ad50172f2faca7689e54

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/kernel-image-2.6.10-6-amd64-generic-di_2.6.10-34.12_i386.deb
Size/MD5: 1467536 82b1e60f723a8ea6fae245a76db240c1

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-headers-2.6.10-6-amd64-generic_2.6.10-34.12_i386.deb
Size/MD5: 287184 ae49ada1414ebd0fbce3a26b81569b0f

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-headers-2.6.10-6-amd64-k8-smp_2.6.10-34.12_i386.deb
Size/MD5: 284004 2b7a790c2edfb6971c2aa8a25f44bb4b

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-headers-2.6.10-6-amd64-k8_2.6.10-34.12_i386.deb
Size/MD5: 286104 e0d26042982a581355296299d329eb1e

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-headers-2.6.10-6-amd64-xeon_2.6.10-34.12_i386.deb
Size/MD5: 281652 c364d465a7ebab2140a11281f55b5c68

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-headers-2.6.10-6_2.6.10-34.12_amd64.deb
Size/MD5: 6138304 2cbef98ab0b63e1609d747f3b228cdc0

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-image-2.6.10-6-amd64-generic_2.6.10-34.12_i386.deb
Size/MD5: 14579418 e77aa9eaab9c0e38639acfb938a0ba69

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-image-2.6.10-6-amd64-k8-smp_2.6.10-34.12_i386.deb
Size/MD5: 15122968 8d225786e618b3b0bed81a6a884bde2e

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-image-2.6.10-6-amd64-k8_2.6.10-34.12_i386.deb
Size/MD5: 15091612 1390444032407b2ec08e9f67707c0136

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-image-2.6.10-6-amd64-xeon_2.6.10-34.12_i386.deb
Size/MD5: 14963420 5b723b3d9ce9165c73934e88fc94436b

[Full-disclosure] [USN-263-1] Linux kernel vulnerabilities

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-patch-ubuntu-2.6.10_2.6.10-34.12_amd64
Size/MD5: 1361302 80232743c254134f3e0ed36550c79929

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/loop-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_amd64
Size/MD5: 14228 8d70a853427d6efc362b8aeb01ae7846

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/md-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_amd64
Size/MD5: 178508 a18ef49481d10939b12b79440294a1b7

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/nfs-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_amd64
Size/MD5: 174888 9d7db26d3c570110ebc7dbc2a6f03b6e

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/nic-extra-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_amd64
Size/MD5: 731208 e73ed9411c4e8c63be93dae1f198834a

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/nic-firmware-2.6.10-6-amd64-generic-di_2.6.10-34.12_amd64
Size/MD5: 780900 84abf1510cc4925f35760d923e060f4e

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/nic-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_amd64
Size/MD5: 150046 174c199cfdfa582e5422a064461125ab

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/nic-pcmcia-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_amd64
Size/MD5: 168120 3026881db2a613fddf2c74c279a52e4e

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/nic-shared-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_amd64
Size/MD5: 9560 6b0ed82f534ae5ea40e202e091b2b09e

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/nic-usb-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_amd64
Size/MD5: 94866 89e0006d8f7c2c0c602b138bd4c60bc7

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/ntfs-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_amd64
Size/MD5: 45734 0629fa4061b3dd6927624895dab89a8

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/parport-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_amd64
Size/MD5: 33166 a1f41765ab78c12d9911b1be61c7fca5

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/pcmcia-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_amd64
Size/MD5: 55290 8f5c29f6d63c3d794af23ae77b874c5e

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/pcmcia-storage-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_amd64
Size/MD5: 4660 baf0e169a8b9761d1ba622e726cd53eb

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/plip-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_amd64
Size/MD5: 7838 7ace4b7014e8ece0c6771cefc0e20d78

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/ppp-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_amd64
Size/MD5: 53804 13f1ee369d205683f1aaaad7ed120882

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/reiserfs-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_amd64
Size/MD5: 111114 12d32b1898a24cfddf17d37ef534c582

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/rtc-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_amd64
Size/MD5: 10156 e950519e2e6c0fb1565959fbce8ae789

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/sata-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_amd64
Size/MD5: 60470 85f89a669e1bacd0408ab906ac60dfd1

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/scsi-common-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_amd64
Size/MD5: 208568 43ac6e850af971c1f96d19c417ea660a

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/scsi-core-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_amd64
Size/MD5: 69270 4b33e18ea3f3067ce74fd1c046268520

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/scsi-extra-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_amd64
Size/MD5: 394796 a47ba355095893d54ed7d1c32bab63b7

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/scsi-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_amd64
Size/MD5: 294500 7ba8faa6fb3bb5b8c62c771a5d343ff1

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/serial-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_amd64
Size/MD5: 12072 c9280b923c44a8978f7b368f6d842cdb

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/socket-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_amd64
Size/MD5: 22658 42f862744501d50a73e743964a00b01d

http://security.ubuntu.com/ubuntu/pool/universe/l/linux-source-2.6.10/ufs-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_amd64

[Full-disclosure] [USN-263-1] Linux kernel vulnerabilities

Size/MD5: 28808 4a094cb7914ea044063077942577c180

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/usb-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_i386.deb

Size/MD5: 56800 7c974b7582b554eec6725d3b1f44dc4d

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/usb-storage-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_i386.deb

Size/MD5: 34940 83abe29c7560429b2d5db13dd143737a

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/xf86-input-libinput-modules-2.6.10-6-amd64-generic-di_2.6.10-34.12_i386.deb

Size/MD5: 247478 24fa01847b29c0a08180ce16b425bbc6

i386 architecture (x86 compatible Intel/AMD)

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/acpi-modules-2.6.10-6-386-di_2.6.10-34.12_i386.deb

Size/MD5: 18166 3a3fa96a18c729d56d3d96f784dbed2b

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/cdrom-core-modules-2.6.10-6-386-di_2.6.10-34.12_i386.deb

Size/MD5: 44828 a53c484b003c1a8cfe924364c3162f78

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/cdrom-modules-2.6.10-6-386-di_2.6.10-34.12_i386.deb

Size/MD5: 103058 283092719f4e4f946c34983d26da2473

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/ext3-modules-2.6.10-6-386-di_2.6.10-34.12_i386.deb

Size/MD5: 86014 ffcba1a6044059919da0cd536edb059b3

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/fat-modules-2.6.10-6-386-di_2.6.10-34.12_i386.deb

Size/MD5: 29082 4f5938c9bb3840cfe80bf78d125795c6

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/fb-modules-2.6.10-6-386-di_2.6.10-34.12_i386.deb

Size/MD5: 39776 2870d632ba4768eddb631c37fb4d9dea

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/firewire-core-modules-2.6.10-6-386-di_2.6.10-34.12_i386.deb

Size/MD5: 71154 297bef66b8e1501136bbc9ff5fcf0635

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/firmware-modules-2.6.10-6-386-di_2.6.10-34.12_i386.deb

Size/MD5: 5504 02a3ef55e04f6c08bc0fecdb6efbaab2

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/floppy-modules-2.6.10-6-386-di_2.6.10-34.12_i386.deb

Size/MD5: 31586 4dade3d469c0644846be9703d66c2ca1

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/ide-core-modules-2.6.10-6-386-di_2.6.10-34.12_i386.deb

Size/MD5: 52942 56da4d7b9890818dd0f37dd579ffa9d4

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/ide-modules-2.6.10-6-386-di_2.6.10-34.12_i386.deb

Size/MD5: 104470 a1540f4668be5b7545eac3d16b42322b

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/input-modules-2.6.10-6-386-di_2.6.10-34.12_i386.deb

Size/MD5: 38634 7006cd967896975badd9ae18364d628f

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/ipv6-modules-2.6.10-6-386-di_2.6.10-34.12_i386.deb

Size/MD5: 114522 a6351068f3817e47d3f1e906553fbbcb

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/irda-modules-2.6.10-6-386-di_2.6.10-34.12_i386.deb

Size/MD5: 190644 081551251d2263c3982930f84196cfb4

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/jfs-modules-2.6.10-6-386-di_2.6.10-34.12_i386.deb

Size/MD5: 86542 467c12e65362dcb2e2a8ace19db9c44f

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/kernel-image-2.6.10-6-386-di_2.6.10-34.12_i386.deb

Size/MD5: 1390008 d332fe77ca51b1006e01f66d16ee10ba

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-headers-2.6.10-6-386_2.6.10-34.12_i386.deb

Size/MD5: 315604 7a18d79484f760f9a01fa4665ea3e129

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-headers-2.6.10-6-686-smp_2.6.10-34.12_i386.deb

Size/MD5: 311398 1a8bb5010c7b7450516a599bc461f57c

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-headers-2.6.10-6-686_2.6.10-34.12_i386.deb

Size/MD5: 313590 f237b6899c02b6602822b75b2621840a

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-headers-2.6.10-6-k7-smp_2.6.10-34.12_i386.deb

Size/MD5: 311546 014478cb3eb99ed25edc8bd46b4526e6

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-headers-2.6.10-6-k7_2.6.10-34.12_i386.deb

[Full-disclosure] [USN-263-1] Linux kernel vulnerabilities

Size/MD5: 313590 dc991a0ef686817f9044dbb498924ba3
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-headers-2.6.10-6_2.6.10-34.12_i386.deb
Size/MD5: 6135220 b5289f6a48b27b757d6efaadb6fd9110
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-image-2.6.10-6-386_2.6.10-34.12_i386.d
Size/MD5: 15613530 d2f9aa8cc8ad714131829a8ab58dd4ec
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-image-2.6.10-6-686-smp_2.6.10-34.12_i
Size/MD5: 16190660 646bb3f9e840744a8ee32e2da0cb4419
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-image-2.6.10-6-686_2.6.10-34.12_i386.d
Size/MD5: 16608476 829918d45bea5a511a1b39096cc521e0
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-image-2.6.10-6-k7-smp_2.6.10-34.12_i3
Size/MD5: 16302134 32e676a4153770bb447511abc9aa263d
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-image-2.6.10-6-k7_2.6.10-34.12_i386.de
Size/MD5: 16672714 1a5a8aa74b8203eee5f9e06d092a94e2
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/linux-patch-ubuntu-2.6.10_2.6.10-34.12_i386.d
Size/MD5: 1360980 2f23c7a628294a53735f45d0923b1243
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/loop-modules-2.6.10-6-386-di_2.6.10-34.12_i3
Size/MD5: 14078 7be5b7473e3f7c816873c75fc1fa931c
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/md-modules-2.6.10-6-386-di_2.6.10-34.12_i38
Size/MD5: 183204 c44a5bc06ba7d3163e094e12a024aab6
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/nfs-modules-2.6.10-6-386-di_2.6.10-34.12_i38
Size/MD5: 172774 f4f899c94364c436149a35d7b8284905
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.
Size/MD5: 967898 e837d697bee366a93e578c27790f1079
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/nic-firmware-2.6.10-6-386-di_2.6.10-34.12_i3
Size/MD5: 780700 aba6229eaa3ece5d270de0eec73aa3e6
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/nic-modules-2.6.10-6-386-di_2.6.10-34.12_i38
Size/MD5: 140666 689d3f30744c59259337833f9594adad
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/nic-pcmcia-modules-2.6.10-6-386-di_2.6.10-3
Size/MD5: 167944 38f3dc1b4126547eec48d8e8556a44be
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
Size/MD5: 9354 4ebfa7ac1bd40ded660466e15ec9ea58
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/nic-usb-modules-2.6.10-6-386-di_2.6.10-34.12
Size/MD5: 89326 9a258d192f429f2ee370d7556b25d7f6
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/ntfs-modules-2.6.10-6-386-di_2.6.10-34.12_i3
Size/MD5: 48132 bffcdb552d2c6f1d3b5d8ab9a4798c2b
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/parport-modules-2.6.10-6-386-di_2.6.10-34.12
Size/MD5: 30888 30e960c32516e0fb3f7d928418f81a10
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/pcmcia-modules-2.6.10-6-386-di_2.6.10-34.12
Size/MD5: 65902 00a4201999307cbb65882da89cdbae59
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/pcmcia-storage-modules-2.6.10-6-386-di_2.6.1
Size/MD5: 4510 8311fb265cafee0f8f95cc6368f86f25
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/plip-modules-2.6.10-6-386-di_2.6.10-34.12_i3
Size/MD5: 7756 89ebecfc6d4d464cb29ae58a957771aa
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/ppp-modules-2.6.10-6-386-di_2.6.10-34.12_i3
Size/MD5: 50780 557a78bbcd7718baa6ff9f39b1151fe9
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/reiserfs-modules-2.6.10-6-386-di_2.6.10-34.12
Size/MD5: 111590 daa6ad45cf45df007b868fb6185a6d44
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/rtc-modules-2.6.10-6-386-di_2.6.10-34.12_i38
Size/MD5: 9892 888be27383aaaa7c4a12f15ce036997
http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/sata-modules-2.6.10-6-386-di_2.6.10-34.12_i3
Size/MD5: 57156 08b42bd2319b7738d52672e7ae1cf1f9

[Full-disclosure] [USN-263-1] Linux kernel vulnerabilities

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/scsi-common-modules-2.6.10-6-386-di_2.6.10-34.12_i386.deb
Size/MD5: 242030 e783b6a6c2cf547c7f3bca3c03c16973

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/scsi-core-modules-2.6.10-6-386-di_2.6.10-34.12_i386.deb
Size/MD5: 66242 fd44d084bf871b0a753374a6bfd5267e

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/scsi-extra-modules-2.6.10-6-386-di_2.6.10-34.12_i386.deb
Size/MD5: 436604 b03dcad67e1eef31fe5cad1c1031d69d

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/scsi-modules-2.6.10-6-386-di_2.6.10-34.12_i386.deb
Size/MD5: 485672 fb52851bf419d7ee3493a7e7d95b70b7

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/serial-modules-2.6.10-6-386-di_2.6.10-34.12_i386.deb
Size/MD5: 11472 7d1b827c742f089e8fa6e099925828c2

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/socket-modules-2.6.10-6-386-di_2.6.10-34.12_i386.deb
Size/MD5: 21244 f3e28714b0186e59b0a590df4920a1a3

http://security.ubuntu.com/ubuntu/pool/universe/l/linux-source-2.6.10/ufs-modules-2.6.10-6-386-di_2.6.10-34.12_i386.deb
Size/MD5: 29526 76115c2add7ed6e4d66d381003981e72

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/usb-modules-2.6.10-6-386-di_2.6.10-34.12_i386.deb
Size/MD5: 106276 8d6b2cf5e773a542f472c085802f12d4

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/usb-storage-modules-2.6.10-6-386-di_2.6.10-34.12_i386.deb
Size/MD5: 33824 70e5bb26a09c681c63a81fe43423973b

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/xfs-modules-2.6.10-6-386-di_2.6.10-34.12_i386.deb
Size/MD5: 261334 39732aea7fb85d9f9463cb98fc168d02

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_2.6.10-34.12_i386.deb
Size/MD5: 24060 0d4909de35ac3d3b9790ec5bceab0fd9

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/affs-modules-2.6.10-6-power4-di_2.6.10-34.12_i386.deb
Size/MD5: 24062 71bcaef6aec33eb081c8654e0d130e61

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/affs-modules-2.6.10-6-powerpc-di_2.6.10-34.12_i386.deb
Size/MD5: 24050 f1e0a4374497893b331ea2c664d6f8f7

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/cdrom-core-modules-2.6.10-6-power3-di_2.6.10-34.12_i386.deb
Size/MD5: 58286 a4e29158e9d2dc59e992136d7f348702

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/cdrom-core-modules-2.6.10-6-power4-di_2.6.10-34.12_i386.deb
Size/MD5: 58294 83a9673afce3114d38e4803620722931

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/cdrom-core-modules-2.6.10-6-powerpc-di_2.6.10-34.12_i386.deb
Size/MD5: 58270 2fd2fee620861707670fedec9a668683

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/ext2-modules-2.6.10-6-power3-di_2.6.10-34.12_i386.deb
Size/MD5: 30290 4f7d5f6d21d76492f0457875ea7f2f9a

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/ext2-modules-2.6.10-6-power4-di_2.6.10-34.12_i386.deb
Size/MD5: 30288 6354d961a54d367d3c43db748b871702

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/ext2-modules-2.6.10-6-powerpc-di_2.6.10-34.12_i386.deb
Size/MD5: 30270 3e2972655eac95547c7f0b7cd3188309

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/ext3-modules-2.6.10-6-power3-di_2.6.10-34.12_i386.deb
Size/MD5: 109252 7d9d5495e90753eba48caaf259e3454e

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/ext3-modules-2.6.10-6-power4-di_2.6.10-34.12_i386.deb
Size/MD5: 109248 9b639c259d1215c4cb078c67fc3565a3

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/ext3-modules-2.6.10-6-powerpc-di_2.6.10-34.12_i386.deb
Size/MD5: 109230 88c265e24cd415efc0e8512aa2c00a22

http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.10/fat-modules-2.6.10-6-power3-di_2.6.10-34.12_i386.deb
Size/MD5: 35388 51467ac08173b8ec362297fe44a9e5e4

[ht](#)