

# [USN-103-1] Linux kernel vulnerabilities

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2005-04/0019.html>

---

**From:** Martin Pitt ([martin.pitt\\_at\\_canonical.com](mailto:martin.pitt_at_canonical.com))

**Date:** 04/01/05

Date: Fri, 1 Apr 2005 10:14:40 +0200

To: [ubuntu-security-announce@lists.ubuntu.com](mailto:ubuntu-security-announce@lists.ubuntu.com)

---

Ubuntu Security Notice USN-103-1 April 01, 2005

linux-source-2.6.8.1 vulnerabilities

CAN-2005-0400, CAN-2005-0749, CAN-2005-0750, CAN-2005-0815,

CAN-2005-0839

---

A security issue affects the following Ubuntu releases:

Ubuntu 4.10 (Warty Warthog)

The following packages are affected:

linux-image-2.6.8.1-5-386  
linux-image-2.6.8.1-5-686  
linux-image-2.6.8.1-5-686-smp  
linux-image-2.6.8.1-5-amd64-generic  
linux-image-2.6.8.1-5-amd64-k8  
linux-image-2.6.8.1-5-amd64-k8-smp  
linux-image-2.6.8.1-5-amd64-xeon  
linux-image-2.6.8.1-5-k7  
linux-image-2.6.8.1-5-k7-smp  
linux-image-2.6.8.1-5-power3  
linux-image-2.6.8.1-5-power3-smp  
linux-image-2.6.8.1-5-power4  
linux-image-2.6.8.1-5-power4-smp  
linux-image-2.6.8.1-5-powerpc  
linux-image-2.6.8.1-5-powerpc-smp  
linux-patch-debian-2.6.8.1

The problem can be corrected by upgrading the affected package to version 2.6.8.1-16.13. You need to reboot the computer after doing a standard system upgrade to effect the necessary changes.

Details follow:

## SecurityFocus Bugtraq: [USN-103-1] Linux kernel vulnerabilities

Mathieu Lafon discovered an information leak in the ext2 file system driver. When a new directory was created, the ext2 block written to disk was not initialized, so that previous memory contents (which could contain sensitive data like passwords) became visible on the raw device. This is particularly important if the target device is removable and thus can be read by users other than root.

(CAN-2005-0400)

Yichen Xie discovered a Denial of Service vulnerability in the ELF loader. A specially crafted ELF library or executable could cause an attempt to free an invalid pointer, which lead to a kernel crash.

(CAN-2005-0749)

Ilja van Sprundel discovered that the bluez\_sock\_create() function did not check its "protocol" argument for negative values. A local attacker could exploit this to execute arbitrary code with root privileges by creating a Bluetooth socket with a specially crafted protocol number. (CAN-2005-0750)

Michal Zalewski discovered that the iso9660 file system driver fails to check ranges properly in several cases. Mounting a specially crafted CD-ROM may have caused a buffer overflow leading to a kernel crash or even arbitrary code execution. (CAN-2005-0815)

Previous kernels did not restrict the use of the N\_MOUSE line discipline in the serial driver. This allowed an unprivileged user to inject mouse movement and/or keystrokes (using the sunkbd driver) into the input subsystem, taking over the console or an X session, where another user is logged in. (CAN-2005-0839)

A Denial of Service vulnerability was found in the tmpfs driver, which is commonly used to mount RAM disks below /dev/shm and /tmp. The shm\_nopage() did not properly verify its address argument, which could be exploited by a local user to cause a kernel crash with invalid addresses.

([http://linux.bkbits.net:8080/linux-2.6/cset@420551fbRlv9-QG6Gw9Lw\\_bKVfPSsg](http://linux.bkbits.net:8080/linux-2.6/cset@420551fbRlv9-QG6Gw9Lw_bKVfPSsg))

Source archives:

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-source-2.6.8.1\\_2.6.8.1-16.13.diff.gz](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-source-2.6.8.1_2.6.8.1-16.13.diff.gz)  
Size/MD5: 3141166 21bb3cb0cb3411b0fc6ed4b193cc5ade

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-source-2.6.8.1\\_2.6.8.1-16.13.dsc](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-source-2.6.8.1_2.6.8.1-16.13.dsc)  
Size/MD5: 2121 c8109995552dbdf33155366c8b6ca574

[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](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\\_2.6.8.1-16.13\\_all.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-doc-2.6.8.1_2.6.8.1-16.13_all.deb)  
Size/MD5: 6156316 ced249a61a235b9954d1ae968e2cb7ca

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-patch-debian-2.6.8.1\\_2.6.8.1-16.13\\_all](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-patch-debian-2.6.8.1_2.6.8.1-16.13_all)

## SecurityFocus Bugtraq: [USN-103-1] Linux kernel vulnerabilities

Size/MD5: 1496926 406d8a710e1d9f95b0c8448962e3f4b7

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-source-2.6.8.1\\_2.6.8.1-16.13\\_all.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-source-2.6.8.1_2.6.8.1-16.13_all.deb)

Size/MD5: 36719760 2b56398fcfbcd6d757a968a552820d5

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-tree-2.6.8.1\\_2.6.8.1-16.13\\_all.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-tree-2.6.8.1_2.6.8.1-16.13_all.deb)

Size/MD5: 308292 5f63ff191ca41e39166de2bd53f8d08c

amd64 architecture (Athlon64, Opteron, EM64T Xeon)

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-amd64-generic\\_2.6.8.1-16.13\\_all.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-amd64-generic_2.6.8.1-16.13_all.deb)

Size/MD5: 247868 21ff61252c900e9fb2a548f30c819789

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-amd64-k8-smp\\_2.6.8.1-16.13\\_all.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-amd64-k8-smp_2.6.8.1-16.13_all.deb)

Size/MD5: 243858 dfda5b8d4eb53ef56e40dacea6c93379

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-amd64-k8\\_2.6.8.1-16.13\\_all.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-amd64-k8_2.6.8.1-16.13_all.deb)

Size/MD5: 247076 21c0419cd1548273b52a141ab145834d

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-amd64-xeon\\_2.6.8.1-16.13\\_all.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-amd64-xeon_2.6.8.1-16.13_all.deb)

Size/MD5: 242192 011e30a52dda6f020df9c643988102d1

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5\\_2.6.8.1-16.13\\_amd64-generic\\_2.6.8.1-16.13\\_all.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5_2.6.8.1-16.13_amd64-generic_2.6.8.1-16.13_all.deb)

Size/MD5: 3179188 ba617aee377d068ce18f21ac6c89263c

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-amd64-generic\\_2.6.8.1-16.13\\_all.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-amd64-generic_2.6.8.1-16.13_all.deb)

Size/MD5: 14353262 1f3ec89ac23adf217960ed38e5d2c717

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-amd64-k8-smp\\_2.6.8.1-16.13\\_all.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-amd64-k8-smp_2.6.8.1-16.13_all.deb)

Size/MD5: 14829032 51dc56cced6815922749538fbd115b2

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-amd64-k8\\_2.6.8.1-16.13\\_all.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-amd64-k8_2.6.8.1-16.13_all.deb)

Size/MD5: 14861698 89eb699bc0e6c2424dd5fe9c3eabf811

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-amd64-xeon\\_2.6.8.1-16.13\\_all.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-amd64-xeon_2.6.8.1-16.13_all.deb)

Size/MD5: 14686210 d3b50f9f86afaa8865b30d57d6b0fa1d

i386 architecture (x86 compatible Intel/AMD)

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-386\\_2.6.8.1-16.13\\_all.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-386_2.6.8.1-16.13_all.deb)

Size/MD5: 277290 c3e00f0ff221ec660319606a4d19e9da

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-686-smp\\_2.6.8.1-16.13\\_all.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-686-smp_2.6.8.1-16.13_all.deb)

Size/MD5: 271980 d1cc69e7b158ee25af65f31675943631

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-686\\_2.6.8.1-16.13\\_all.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-686_2.6.8.1-16.13_all.deb)

Size/MD5: 275018 17561ffd0e1448df572350eeba6cdb0d

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-k7-smp\\_2.6.8.1-16.13\\_all.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-k7-smp_2.6.8.1-16.13_all.deb)

Size/MD5: 272506 0cd5266261e4a4695c0f4613562c6cc3

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-k7\\_2.6.8.1-16.13\\_all.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-k7_2.6.8.1-16.13_all.deb)

Size/MD5: 275150 729e035be50a7315f9b6484a2127755b

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5\\_2.6.8.1-16.13\\_i386-generic\\_2.6.8.1-16.13\\_all.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5_2.6.8.1-16.13_i386-generic_2.6.8.1-16.13_all.deb)

Size/MD5: 3219988 f89b979f9ca5aa2be0f24dca74270810

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-386\\_2.6.8.1-16.13\\_i386-generic\\_2.6.8.1-16.13\\_all.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-386_2.6.8.1-16.13_i386-generic_2.6.8.1-16.13_all.deb)

Size/MD5: 15495380 5b4a074ba11309dd403d300e01ca5d42

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-686-smp\\_2.6.8.1-16.13\\_all.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-686-smp_2.6.8.1-16.13_all.deb)

Size/MD5: 16345080 ee2b9c141d287b4606fe6b1d23ed3c76

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-686\\_2.6.8.1-16.13\\_i386-generic\\_2.6.8.1-16.13\\_all.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-686_2.6.8.1-16.13_i386-generic_2.6.8.1-16.13_all.deb)

Size/MD5: 16513718 1e3cff372acdfc294063e0a2e8ef485

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-k7-smp\\_2.6.8.1-16.13\\_all.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-k7-smp_2.6.8.1-16.13_all.deb)

Size/MD5: 16447908 21dfa2d945203fcb5d9d9385ee86c659

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-k7\\_2.6.8.1-16.13\\_i386-generic\\_2.6.8.1-16.13\\_all.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-k7_2.6.8.1-16.13_i386-generic_2.6.8.1-16.13_all.deb)

Size/MD5: 16573202 d7440b858e2b88b56ada1fd9c3aef045

## SecurityFocus Bugtraq: [USN-103-1] Linux kernel vulnerabilities

powerpc architecture (Apple Macintosh G3/G4/G5)

<http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-power3-smp> 2.6.8.1-5-power3-smp  
Size/MD5: 212896 70301c701acd9e1d0682d664e63479c7

<http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-power3> 2.6.8.1-16.13-power3  
Size/MD5: 213610 3de6832705d851b4762a677ae7efcfe3

<http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-power4-smp> 2.6.8.1-5-power4-smp  
Size/MD5: 212694 79dcc690556561c7f6b2835cadaefc65

<http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-power4> 2.6.8.1-16.13-power4  
Size/MD5: 213368 fccda4ef54e82ef7bc9ee65dd91ad9f2

<http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-powerpc-smp> 2.6.8.1-5-powerpc-smp  
Size/MD5: 213274 cb5c15759fdc1c3d67dea083fa715425

<http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-powerpc> 2.6.8.1-16.13-powerpc  
Size/MD5: 214772 738757d77bb43291937bbb8fa8e5279b

<http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5> 2.6.8.1-16.13-powerpc  
Size/MD5: 3297198 c449b6f307be309b4b34096067854afd

<http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-power3-smp> 2.6.8.1-5-power3-smp  
Size/MD5: 16367564 e989eb486e57f3fdf01ba02f9aed6e5d

<http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-power3> 2.6.8.1-16.13-power3  
Size/MD5: 15942266 a3c8ed4b84d39219124c4ea70caef211

<http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-power4-smp> 2.6.8.1-5-power4-smp  
Size/MD5: 16354794 6c528b50c53088c14353845e609bc868

<http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-power4> 2.6.8.1-16.13-power4  
Size/MD5: 15926402 2210381c424e430a48e2579226ae9fca

<http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-powerpc-smp> 2.6.8.1-5-powerpc-smp  
Size/MD5: 16289246 4fd1a22f145d0abdc84e8926dfa42df8

<http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-powerpc> 2.6.8.1-16.13-powerpc  
Size/MD5: 15975494 3424a2f8dc666e9520c5abc929b08e62

- 
- application/pgp-signature attachment: Digital signature