

# [Full-disclosure] [USN-95-1] Linux kernel vulnerabilities

**Source:** <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-03/0534.html>

---

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

**Date:** 03/15/05

Date: Tue, 15 Mar 2005 15:12:28 +0100

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

=====  
Ubuntu Security Notice USN-95-1 March 15, 2005

linux-source-2.6.8.1 vulnerabilities

CAN-2005-0209, CAN-2005-0210, CAN-2005-0384, CAN-2005-0529,

CAN-2005-0530, CAN-2005-0531, CAN-2005-0532, CAN-2005-0736  
=====

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 2.6.8.1-16.12. You need to reboot the computer after doing a standard system upgrade to effect the necessary changes.

## Full-Disclosure: [Full-disclosure] [USN-95-1] Linux kernel vulnerabilities

Details follow:

A remote Denial of Service vulnerability was discovered in the Netfilter IP packet handler. This allowed a remote attacker to crash the machine by sending specially crafted IP packet fragments. (CAN-2005-0209)

The Netfilter code also contained a memory leak. Certain locally generated packet fragments are reassembled twice, which caused a double allocation of a data structure. This could be locally exploited to crash the machine due to kernel memory exhaustion. (CAN-2005-0210)

Ben Martel and Stephen Blackheath found a remote Denial of Service vulnerability in the PPP driver. This allowed a malicious pppd client to crash the server machine. (CAN-2005-0384)

Georgi Guninski discovered a buffer overflow in the ATM driver. The atm\_get\_addr() function does not validate its arguments sufficiently, which could allow a local attacker to overwrite large portions of kernel memory by supplying a negative length argument. This could eventually lead to arbitrary code execution. (CAN-2005-0531)

Georgi Guninski also discovered three other integer comparison problems in the TTY layer, in the /proc interface and the ReiserFS driver. However, the previous Ubuntu security update (kernel version 2.6.8.1-16.11) already contained a patch which checks the arguments to these functions at a higher level and thus prevents these flaws from being exploited. (CAN-2005-0529, CAN-2005-0530, CAN-2005-0532)

Georgi Guninski discovered an integer overflow in the sys\_epoll\_wait() function which allowed local users to overwrite the first few kB of physical memory. However, very few applications actually use this space (dosemu is a notable exception), but potentially this could lead to privilege escalation. (CAN-2005-0736)

Eric Anholt discovered a race condition in the Radeon DRI driver. In some cases this allowed a local user with DRI privileges on a Radeon card to execute arbitrary code with root privileges.

Finally this update fixes a regression in the NFS server driver which was introduced in the previous security update (kernel version 2.6.8.1-16.11). We apologize for the inconvenience. ([https://bugzilla.ubuntulinux.org/show\\_bug.cgi?id=6749](https://bugzilla.ubuntulinux.org/show_bug.cgi?id=6749))

Source archives:

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-source-2.6.8.1\\_2.6.8.1-16.12.diff.gz](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-source-2.6.8.1_2.6.8.1-16.12.diff.gz)  
Size/MD5: 3138173 562c678c1db3839022a46fe6707b17a2

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-source-2.6.8.1\\_2.6.8.1-16.12.dsc](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-source-2.6.8.1_2.6.8.1-16.12.dsc)  
Size/MD5: 2121 ca9878e5a4300fb3d3ae973528826752

[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)

## Full-Disclosure: [Full-disclosure] [USN-95-1] Linux kernel vulnerabilities

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\\_2.6.8.1-16.12\\_all.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-doc-2.6.8.1_2.6.8.1-16.12_all.deb)  
Size/MD5: 6156398 8c909af9ca59a3ca9332e9b104550345

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-patch-debian-2.6.8.1\\_2.6.8.1-16.12\\_all.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-patch-debian-2.6.8.1_2.6.8.1-16.12_all.deb)  
Size/MD5: 1494402 7a0837f2bf959a81c654c739adbd46e9

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-source-2.6.8.1\\_2.6.8.1-16.12\\_all.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-source-2.6.8.1_2.6.8.1-16.12_all.deb)  
Size/MD5: 36720352 05befe6c04d9327f92b49f8141220449

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-tree-2.6.8.1\\_2.6.8.1-16.12\\_all.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-tree-2.6.8.1_2.6.8.1-16.12_all.deb)  
Size/MD5: 308034 147891a0041bcf9d210915a71914d6c0

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\\_2.6.8.1-16.12\\_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_2.6.8.1-16.12_all.deb)  
Size/MD5: 247896 7dd57b2064006690e2cdcad73ee68d45

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-amd64-k8-smp\\_2.6.8.1-16.12\\_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_2.6.8.1-16.12_all.deb)  
Size/MD5: 243798 af368e29fd8253726f4d98fc61ae8e63

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-amd64-k8\\_2.6.8.1-16.12\\_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_2.6.8.1-16.12_all.deb)  
Size/MD5: 246918 2f15a30e62829856a793e1750d1627ec

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-amd64-xeon\\_2.6.8.1-16.12\\_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_2.6.8.1-16.12_all.deb)  
Size/MD5: 242064 095a0823406b09537441e3e57bc2ab6c

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5\\_2.6.8.1-16.12\\_amd64.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5_2.6.8.1-16.12_amd64.deb)  
Size/MD5: 3178994 b3837998e2015412d6a23a1767ab1f11

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-amd64-generic\\_2.6.8.1-16.12\\_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_2.6.8.1-16.12_all.deb)  
Size/MD5: 14352688 c5be7b5e81a224bbe32c96f8abb4612e

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-amd64-k8-smp\\_2.6.8.1-16.12\\_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_2.6.8.1-16.12_all.deb)  
Size/MD5: 14828788 eb195f0cf157bfe5da0dc5b77b156c27

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-amd64-k8\\_2.6.8.1-16.12\\_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_2.6.8.1-16.12_all.deb)  
Size/MD5: 14861436 b43ddb164a0a2cc8808d1262b8d5750d

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-amd64-xeon\\_2.6.8.1-16.12\\_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_2.6.8.1-16.12_all.deb)  
Size/MD5: 14684670 3420b9272177aece4bde1a566e894cf2

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\\_2.6.8.1-16.12\\_all.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-386_2.6.8.1-16.12_all.deb)  
Size/MD5: 276950 3d9f318befd4cabac0f059a85c06324c0

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-686-smp\\_2.6.8.1-16.12\\_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_2.6.8.1-16.12_all.deb)  
Size/MD5: 271656 09e1b2b404a079852f81b4d7b6eae7bb

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-686\\_2.6.8.1-16.12\\_all.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-686_2.6.8.1-16.12_all.deb)  
Size/MD5: 274682 9f5ae2ee5d09e85f799eaf4ea3770615

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-k7-smp\\_2.6.8.1-16.12\\_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_2.6.8.1-16.12_all.deb)  
Size/MD5: 272144 67499c9baf38440ee8f3f2b09b667e8

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-k7\\_2.6.8.1-16.12\\_i386.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-k7_2.6.8.1-16.12_i386.deb)  
Size/MD5: 274840 754e3a4030ee75d3362466832849acbd

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5\\_2.6.8.1-16.12\\_i386.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5_2.6.8.1-16.12_i386.deb)  
Size/MD5: 3219706 508896938223113ea1699aa4151b8766

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-386\\_2.6.8.1-16.12\\_i386.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-386_2.6.8.1-16.12_i386.deb)  
Size/MD5: 15495248 38b990d93eaba078db891bd7404c01e7

[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-686-smp\\_2.6.8.1-16.12\\_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_2.6.8.1-16.12_all.deb)

## Full-Disclosure: [Full-disclosure] [USN-95-1] Linux kernel vulnerabilities

Size/MD5: 16344242 89cb33e659438f4e34b68ba3c32106cd  
[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-686\\_2.6.8.1-16.12\\_i386.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-686_2.6.8.1-16.12_i386.deb)  
Size/MD5: 16512992 4147111c66724fa8691e4b16c356ce86  
[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-k7-smp\\_2.6.8.1-16.12\\_i386.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-k7-smp_2.6.8.1-16.12_i386.deb)  
Size/MD5: 16447442 663241c045b232b8b46ff9c5d5b2f973  
[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-k7\\_2.6.8.1-16.12\\_i386.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-k7_2.6.8.1-16.12_i386.deb)  
Size/MD5: 16572538 8b8891f4526497e43eab0c173f179615

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\\_2.6.8.1-16.12\\_i386.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-power3-smp_2.6.8.1-16.12_i386.deb)  
Size/MD5: 212792 cb39e28e0814976f2831528e20bf8deb  
[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-power3\\_2.6.8.1-16.12\\_i386.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-power3_2.6.8.1-16.12_i386.deb)  
Size/MD5: 213482 5b469307ceb0839a5ca73e170bd4b5a9  
[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-power4-smp\\_2.6.8.1-16.12\\_i386.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-power4-smp_2.6.8.1-16.12_i386.deb)  
Size/MD5: 212514 eec8a75e60edee4eb0784cc44b4c5991  
[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-power4\\_2.6.8.1-16.12\\_i386.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-power4_2.6.8.1-16.12_i386.deb)  
Size/MD5: 213232 7dc2c5a6884dc3bb9e12cb15c2d86475  
[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-powerpc-smp\\_2.6.8.1-16.12\\_i386.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-powerpc-smp_2.6.8.1-16.12_i386.deb)  
Size/MD5: 213112 71c2be933fe1cae5cf04a834af834b97  
[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-powerpc\\_2.6.8.1-16.12\\_i386.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5-powerpc_2.6.8.1-16.12_i386.deb)  
Size/MD5: 214548 72904d0d50787c36b097c11f480329ba  
[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5\\_2.6.8.1-16.12\\_i386.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-headers-2.6.8.1-5_2.6.8.1-16.12_i386.deb)  
Size/MD5: 3297040 15f7b67ca420635504ba90d020cd5990  
[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-power3-smp\\_2.6.8.1-16.12\\_i386.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-power3-smp_2.6.8.1-16.12_i386.deb)  
Size/MD5: 16366562 437904d293401104d04e879394be098e  
[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-power3\\_2.6.8.1-16.12\\_i386.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-power3_2.6.8.1-16.12_i386.deb)  
Size/MD5: 15942190 1b71783b31ec56e29d09dfa8de844caa  
[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-power4-smp\\_2.6.8.1-16.12\\_i386.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-power4-smp_2.6.8.1-16.12_i386.deb)  
Size/MD5: 16353764 8aefa48d5f7461db9ede5fd05da3c57a  
[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-power4\\_2.6.8.1-16.12\\_i386.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-power4_2.6.8.1-16.12_i386.deb)  
Size/MD5: 15924916 14f880d34cd8f1e232ec52a559f046af  
[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-powerpc-smp\\_2.6.8.1-16.12\\_i386.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-powerpc-smp_2.6.8.1-16.12_i386.deb)  
Size/MD5: 16289024 1878256aaff9b8bbb003554590d359b3  
[http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-powerpc\\_2.6.8.1-16.12\\_i386.deb](http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/linux-image-2.6.8.1-5-powerpc_2.6.8.1-16.12_i386.deb)  
Size/MD5: 15975818 8ba319a47d693a063cfae316aaf965e8

---

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://www.secunia.com/>

---

- application/pgp-signature attachment: [Digital signature](#)