

[Full-Disclosure] SUSE Security Announcement: various kernel problems (SUSE-SA:2004:044)

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-12/0533.html>

From: Marcus Meissner (*meissner_at_suse.de*)

Date: 12/21/04

Date: Tue, 21 Dec 2004 20:37:48 +0100

To: full-disclosure@lists.netsys.com

-----BEGIN PGP SIGNED MESSAGE-----

SUSE Security Announcement

Package: kernel

Announcement-ID: SUSE-SA:2004:044

Date: Tuesday, Dec 21st 2004 18:00 MEST

Affected products: SUSE Linux 8.1, 8.2, 9.0, 9.1, 9.2

SUSE Linux Enterprise Server 8, 9

SUSE Linux Desktop 1.0

Novell Linux Desktop 9

Vulnerability Type: local privilege escalation

remote denial of service

local denial of service

Severity (1-10): 9

SUSE default package: yes

Cross References: CAN-2004-1068

CAN-2004-1016

CAN-2004-1137

CAN-2004-1151

Content of this advisory:

- 1) security vulnerability resolved:
 - several vulnerabilities in the linux kernelproblem description
- 2) solution/workaround
- 3) special instructions and notes
- 4) package location and checksums
- 5) pending vulnerabilities, solutions, workarounds:
 - problem with smbfs in earlier update
 - see SUSE Security Summary Report
- 6) standard appendix (further information)

1) problem description, brief discussion

Linux kernel

Several vulnerabilities have been found and fixed in the Linux kernel.

Paul Starzetz reported that the missing serialization in `unix_dgram_recvmsg()` which was added to kernel 2.4.28 can be used by a local attacker to gain elevated privileges (root access). This issue is tracked by the Mitre CVE ID CAN-2004-1068.

Paul Starzetz and Georgi Guninski reported independently that bad argument handling and bad integer arithmetics in the IPv4 `sendmsg` handling of control messages could lead to a local attacker crashing the machine.

This problem was fixed by Herbert Xu and is tracked by the Mitre CVE ID CAN-2004-1016.

Georgi Guninski reported a memory leak in the IP option handling of the IPv4 `sendmsg` call.

Paul Starzetz found bad handling in the kernel IGMP code, which could lead to a local attacker being able to crash the machine. This problem was fixed by Chris Wright and is tracked by the Mitre CVE ID CAN-2004-1137.

Olaf Kirch found and fixed a problem in the RPC handling in the kernel of SUSE Linux 9.1, 9.2, and SUSE Linux Enterprise Server 9 which could lead to a remote attacker crashing the machine.

A local denial of service problem in the `aio_free_ring` system call could allow a local attacker to crash the machine.

A problem in the memory management handling of ELF executables could lead to a local attacker crashing the machine with a handcrafted ELF binary. (This is a VMA overlap problem and not related to earlier ELF problems.)

A buffer overflow in the system call handling in the 32bit system call emulation on AMD64 / Intel EM64T systems was fixed. It is not thought to be exploitable.

A memory leak in the `ip_conntrack_ftp` firewalling module was fixed in the 2.6 kernels.

Various UML security issues in the SUSE Linux 9.2 UML setup were fixed.

Additionally some non-security bugs were fixed in the released kernels:

SUSE Linux Enterprise Server 8 and SUSE Linux 8.1:

- A memory leak in addition / removal of SCSI target devices was fixed.
- A race condition in SCSI I/O accounting which could lead to erroneous reports on SCSI disk I/O was fixed.
- S390: Patches from IBM have been installed in the S/390 architecture, both for 32 and 64bit.
Refer to the maintenance information mail for the full change log.
- The "memfrac" and "lower_zone_reserve" kernel parameters had no effect since they were used before kernel command line parsing.
- PowerPC: Missing synchronization that could lead to processes hanging in signal delivery was added.

SUSE Linux Enterprise Server 9 and SUSE Linux 9.1:

- A vfree() was called with interrupts disabled in the SCSI generic device handling, which could lead to a hanging machine.
- A race condition between a file unlink and umount could lead to a machine crash.
- Fixed a small memory leak in bio_copy_user().
- cdrecord –scanbus could crash the kernel when using the "gdth" SCSI driver.
- Allow reading from zero page (/dev/zero) using O_DIRECT/rawio.
- Fixed some LSB issues in the fcntl compatibility handling.
- The st (SCSI tape) driver did not pass on generic SCSI ioctl commands to the SCSI mid layer.

SUSE Linux 9.2:

- The kernel installation routines did not call depmod for the modules in the –nongpl RPMs, so they could not be loaded.
This lead to non working USB modem drivers and similar.
This problem was fixed.
- A Problem with mounting iPods over FireWire was fixed.
- A data corruption problem in the megaraid driver was fixed.
- A pageattr overflow condition in the memory subsystem and missing TLB flush if multiple pages were passed were fixed.

- Allow reading from zeropage with O_DIRECT/rawio.
- Do not restart the system on ACPI events after power down.
(Make it no longer start on opening the lid of just shutdown laptops for instance.)
- New memory imbalance handling handling by Andrea leading to better Out Of Memory (OOM) handling was added.

2) solution/workaround

Please install the fixed packages, there is no workaround.

3) special instructions and notes

SPECIAL INSTALL INSTRUCTIONS:

=====

The following paragraphs will guide you through the installation process in a step-by-step fashion. The character sequence "****" marks the beginning of a new paragraph. In some cases, the steps outlined in a particular paragraph may or may not be applicable to your situation.

Therefore, please make sure to read through all of the steps below before attempting any of these procedures.

All of the commands that need to be executed are required to be run as the superuser (root). Each step relies on the steps before it to complete successfully.

**** Step 1: Determine the needed kernel type

Please use the following command to find the kernel type that is installed on your system:

```
rpm -qf /boot/vmlinuz
```

Following are the possible kernel types (disregard the version and build number following the name separated by the "-" character)

```
k_deflt # default kernel, good for most systems.  
k_i386 # kernel for older processors and chip sets  
k_athlon # kernel made specifically for AMD Athlon(tm) family processors  
k_psmpp # kernel for Pentium-I dual processor systems  
k_smp # kernel for SMP systems (Pentium-II and above)  
k_smp4G # kernel for SMP systems which supports a maximum of 4G of RAM  
kernel-64k-pagesize  
kernel-bigsmp  
kernel-default  
kernel-smp
```

**** Step 2: Download the package for your system

Please download the kernel RPM package for your distribution with the name as indicated by Step 1. The list of all kernel rpm packages is appended below. Note: The kernel-source package does not contain a binary kernel in bootable form. Instead, it contains the sources that the binary kernel rpm packages are created from. It can be used by administrators who have decided to build their own kernel. Since the kernel-source.rpm is an installable (compiled) package that contains sources for the linux kernel, it is not the source RPM for the kernel RPM binary packages.

The kernel RPM binary packages for the distributions can be found at the locations below <ftp://ftp.suse.com/pub/suse/i386/update/>.

8.1/rpm/i586
8.2/rpm/i586
9.0/rpm/i586
9.1/rpm/i586
9.2/rpm/i586

After downloading the kernel RPM package for your system, you should verify the authenticity of the kernel rpm package using the methods as listed in section 3) of each SUSE Security Announcement.

**** Step 3: Installing your kernel rpm package

Install the rpm package that you have downloaded in Steps 3 or 4 with the command

```
rpm -Uhv --nodeps --force <K_FILE.RPM>
```

where <K_FILE.RPM> is the name of the rpm package that you downloaded.

Warning: After performing this step, your system will likely not be able to boot if the following steps have not been fully followed.

If you run SUSE LINUX 8.1 and haven't applied the kernel update (SUSE-SA:2003:034), AND you are using the freeswan package, you also need to update the freeswan rpm as a dependency as offered by YOU (YaST Online Update). The package can be downloaded from <ftp://ftp.suse.com/pub/suse/i386/update/8.1/rpm/i586/>

**** Step 4: configuring and creating the initrd

The initrd is a ramdisk that is loaded into the memory of your system together with the kernel boot image by the bootloader. The kernel uses the content of this ramdisk to execute commands that must be run before the kernel can mount its actual root filesystem. It is usually used to initialize SCSI drivers or NIC drivers for diskless operation.

The variable INITRD_MODULES in /etc/sysconfig/kernel determines which kernel modules will be loaded in the initrd before the kernel

has mounted its actual root filesystem. The variable should contain your SCSI adapter (if any) or filesystem driver modules.

With the installation of the new kernel, the `initrd` has to be re-packed with the update kernel modules. Please run the command

```
mk_initrd
```

as root to create a new init ramdisk (`initrd`) for your system.

On SuSE Linux 8.1 and later, this is done automatically when the RPM is installed.

**** Step 5: bootloader

If you run a SUSE LINUX 8.x, SLES8, or SUSE LINUX 9.x system, there are two options:

Depending on your software configuration, you have either the lilo bootloader or the grub bootloader installed and initialized on your system.

The grub bootloader does not require any further actions to be performed after the new kernel images have been moved in place by the `rpm Update` command.

If you have a lilo bootloader installed and initialized, then the lilo program must be run as root. Use the command

```
grep LOADER_TYPE /etc/sysconfig/bootloader
```

to find out which boot loader is configured. If it is lilo, then you must run the lilo command as root. If grub is listed, then your system does not require any bootloader initialization.

Warning: An improperly installed bootloader may render your system unbootable.

**** Step 6: reboot

If all of the steps above have been successfully completed on your system, then the new kernel including the kernel modules and the `initrd` should be ready to boot. The system needs to be rebooted for the changes to become active. Please make sure that all steps have completed, then reboot using the command

```
shutdown -r now
```

or

```
init 6
```

Your system should now shut down and reboot with the new kernel.

4) package location and checksums

Please download the update package for your distribution and verify its integrity by the methods listed in section 3) of this announcement.

Then, install the package using the command "rpm -Fhv file.rpm" to apply the update.

Our maintenance customers are being notified individually. The packages are being offered to install from the maintenance web.

x86 Platform:

SUSE Linux 9.2:

<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/i586/kernel-source-2.6.8-24.8.i586.rpm>
8dc5b70f5fdef7c0437372d2811bcb02

<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/i586/kernel-default-2.6.8-24.8.i586.rpm>
134c37732850c86ef872c97171c81ede

<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/i586/kernel-smp-2.6.8-24.8.i586.rpm>
f552ef1f49675a4e8dc8f71ad7829ed1

<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/i586/kernel-bigsmp-2.6.8-24.8.i586.rpm>
ea2be2b3152a5b6d362636cc29534007

<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/i586/kernel-default-nongpl-2.6.8-24.8.i586.rpm>
f5af05e9e7ec387fe1ce755b8f53a022

<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/i586/kernel-smp-nongpl-2.6.8-24.8.i586.rpm>
94e01d31f7cdda2a2ae00377613ad625

<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/i586/kernel-bigsmp-nongpl-2.6.8-24.8.i586.rpm>
f3437bd22be65df11df36b9722f15fa7

<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/i586/um-host-kernel-2.6.8-24.8.i586.rpm>
772e6200300a11d137383e51486cd159

<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/i586/um-host-install-initrd-1.0-48.3.i586.rpm>
00eba31f6adc46309c4be34ddd477d1a

patch rpm(s):

<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/i586/um-host-kernel-2.6.8-24.8.i586.patch.rpm>
00d6b04af9b54eaff147d7267d66ae08

<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/i586/um-host-install-initrd-1.0-48.3.i586.patch.rpm>
2de74bf6f185d1c732412945147c4914

source rpm(s):

<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/src/kernel-source-2.6.8-24.8.src.rpm>
bc9e4a08ba429884716d9e1768ca7391

<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/src/kernel-default-2.6.8-24.8.nosrc.rpm>
0cbc4714154be7df7a18fda4c5ca595b

<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/src/kernel-smp-2.6.8-24.8.nosrc.rpm>
451d4c51a5d4083b4e663913bb53e622

<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/src/kernel-bigsmp-2.6.8-24.8.nosrc.rpm>
292bc1aab35f113099765e01f5c87b8e

<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/src/kernel-default-2.6.8-24.8.nosrc.rpm>
0cbc4714154be7df7a18fda4c5ca595b

<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/src/kernel-smp-2.6.8-24.8.nosrc.rpm>
451d4c51a5d4083b4e663913bb53e622

<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/src/kernel-bigsmp-2.6.8-24.8.nosrc.rpm>
292bc1aab35f113099765e01f5c87b8e

<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/src/kernel-um-2.6.8-24.8.nosrc.rpm>
32aeaea2ff952d83cfd2cf94b1358d33

<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/src/um-host-install-initrd-1.0-48.3.src.rpm>
bc079272affb6c4a444ff0eed5668c58

SUSE Linux 9.1:

<ftp://ftp.suse.com/pub/suse/i386/update/9.1/rpm/i586/kernel-source-2.6.5-7.111.19.i586.rpm>
b5905fea74dd7c6b43896506c28a23d7

<ftp://ftp.suse.com/pub/suse/i386/update/9.1/rpm/i586/kernel-default-2.6.5-7.111.19.i586.rpm>
35fd6f0047d3666f6402b07175c69ce2

<ftp://ftp.suse.com/pub/suse/i386/update/9.1/rpm/i586/kernel-smp-2.6.5-7.111.19.i586.rpm>
0a41cb4c8a9325b15ffee9407af62e08

<ftp://ftp.suse.com/pub/suse/i386/update/9.1/rpm/i586/kernel-bigsmmp-2.6.5-7.111.19.i586.rpm>
4cc0c401f76b7d5109dfbd7e2775c83f

source rpm(s):

<ftp://ftp.suse.com/pub/suse/i386/update/9.1/rpm/src/kernel-source-2.6.5-7.111.19.src.rpm>
cbfd74fdb9bb2c9017f281a7ffe3ea0c

<ftp://ftp.suse.com/pub/suse/i386/update/9.1/rpm/src/kernel-default-2.6.5-7.111.19.nosrc.rpm>
11708c86166aff33fe48157d998139a3

<ftp://ftp.suse.com/pub/suse/i386/update/9.1/rpm/src/kernel-smp-2.6.5-7.111.19.nosrc.rpm>
5989481ab5506a2a8ee539b172fd3a3e

<ftp://ftp.suse.com/pub/suse/i386/update/9.1/rpm/src/kernel-bigsmmp-2.6.5-7.111.19.nosrc.rpm>
25e8246b9d18d6bac0087ccd16012c8b

SUSE Linux 9.0:

<ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/i586/kernel-source-2.4.21-266.i586.rpm>
3fab8709c6f108985e6db14d8eddd68

<ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/i586/kernel-default-2.4.21-266.i586.rpm>
d7d5f9d018ed62aa4785046128509de7

<ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/i586/kernel-smp-2.4.21-266.i586.rpm>
151eec47b73e0aab0376a8d4dd108607

<ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/i586/kernel-athlon-2.4.21-266.i586.rpm>
ea1f74c173b2fac8bc5a335de2304e3f

source rpm(s):

<ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/src/kernel-source-2.4.21-266.src.rpm>
06dea7c190f66312cee81b9d59f6b968

<ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/src/kernel-default-2.4.21-266.src.rpm>
63b4cdc0ef1549057931da01b3ebc1a3

<ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/src/kernel-smp-2.4.21-266.src.rpm>
1636bcd52054dd60493def485fa00576

<ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/src/kernel-athlon-2.4.21-266.src.rpm>
0f2ab3b06dc3be82a31317cece16ad7b

SUSE Linux 8.2:

<ftp://ftp.suse.com/pub/suse/i386/update/8.2/rpm/i586/kernel-source-2.4.20.SuSE-127.i586.rpm>
1baebbe7215434dec73aeaec61b68579

<ftp://ftp.suse.com/pub/suse/i386/update/8.2/rpm/i586/kernel-default-2.4.20-127.i586.rpm>
500299c75a582d4ac4fb9d9d56e6ce9d

<ftp://ftp.suse.com/pub/suse/i386/update/8.2/rpm/i586/kernel-smp-2.4.20-127.i586.rpm>
6cee78e7216c8fa9b07a5b78c7a0b774

<ftp://ftp.suse.com/pub/suse/i386/update/8.2/rpm/i586/kernel-athlon-2.4.20-127.i586.rpm>
e15fe145d9d62977f89f3647d43d6692

<ftp://ftp.suse.com/pub/suse/i386/update/8.2/rpm/i586/kernel-psmp-2.4.20-127.i586.rpm>
a88e3cd46a56f49f4846d151a05d4430

source rpm(s):

<ftp://ftp.suse.com/pub/suse/i386/update/8.2/rpm/src/kernel-source-2.4.20.SuSE-127.src.rpm>

bd4ba934e3ce4dec888fcdf26e5dec38
ftp://ftp.suse.com/pub/suse/i386/update/8.2/rpm/src/k_deflt-2.4.20-127.src.rpm
c1e43e827b7d2db8d0a189daf33c3eee
ftp://ftp.suse.com/pub/suse/i386/update/8.2/rpm/src/k_smp-2.4.20-127.src.rpm
3871dac3965594d5e368fd91f56f07cb
ftp://ftp.suse.com/pub/suse/i386/update/8.2/rpm/src/k_athlon-2.4.20-127.src.rpm
74d66b02ab0cadb0cc6709068f30e7e5
ftp://ftp.suse.com/pub/suse/i386/update/8.2/rpm/src/k_psmpp-2.4.20-127.src.rpm
318b66cbf216317af917bc8e7cc28fea

SUSE Linux 8.1:

<ftp://ftp.suse.com/pub/suse/i386/update/8.1/rpm/i586/kernel-source-2.4.21-266.i586.rpm>
496f775186fb745b86e7545e9f13e7bd
ftp://ftp.suse.com/pub/suse/i386/update/8.1/rpm/i586/k_deflt-2.4.21-266.i586.rpm
174fd559a0378e35aa11fb2d93a2684b
ftp://ftp.suse.com/pub/suse/i386/update/8.1/rpm/i586/k_smp-2.4.21-266.i586.rpm
add6505218c8f6929d79305ee7343727
ftp://ftp.suse.com/pub/suse/i386/update/8.1/rpm/i586/k_athlon-2.4.21-266.i586.rpm
3cc4344755df9721d20d717a0ff2ecc4
ftp://ftp.suse.com/pub/suse/i386/update/8.1/rpm/i586/k_psmpp-2.4.21-266.i586.rpm
a2b0cb0c0181f4dc5a072e21789dc585

source rpm(s):

<ftp://ftp.suse.com/pub/suse/i386/update/8.1/rpm/src/kernel-source-2.4.21-266.src.rpm>
40d6ed2f4c77f2225bed7a5dd7f8e346
ftp://ftp.suse.com/pub/suse/i386/update/8.1/rpm/src/k_deflt-2.4.21-266.src.rpm
70e9a1131849f3d98c8d5009915abb52
ftp://ftp.suse.com/pub/suse/i386/update/8.1/rpm/src/k_smp-2.4.21-266.src.rpm
b7eb4f46bd06cab9aa1ad7c97264c96c
ftp://ftp.suse.com/pub/suse/i386/update/8.1/rpm/src/k_athlon-2.4.21-266.src.rpm
66879d8b6ffff23e44895bbfa6c1c644
ftp://ftp.suse.com/pub/suse/i386/update/8.1/rpm/src/k_psmpp-2.4.21-266.src.rpm
ade3afd2816ba005650b82de9dc1da7b

x86-64 Platform:

SUSE Linux 9.2:

ftp://ftp.suse.com/pub/suse/x86_64/update/9.2/rpm/x86_64/kernel-source-2.6.8-24.8.x86_64.rpm
dca3907a9c0e31ea7fd3cb13f6d7a2c7
ftp://ftp.suse.com/pub/suse/x86_64/update/9.2/rpm/x86_64/kernel-default-2.6.8-24.8.x86_64.rpm
22d4f74fe29eae1acb8a4daced16c26
ftp://ftp.suse.com/pub/suse/x86_64/update/9.2/rpm/x86_64/kernel-smp-2.6.8-24.8.x86_64.rpm
b38935409955a9f7e427532f1a9a110e
ftp://ftp.suse.com/pub/suse/x86_64/update/9.2/rpm/x86_64/kernel-default-nongpl-2.6.8-24.8.x86_64.rpm
a4196f62b128a4d59106b6e4fb91a89d
ftp://ftp.suse.com/pub/suse/x86_64/update/9.2/rpm/x86_64/kernel-smp-nongpl-2.6.8-24.8.x86_64.rpm
7ab6d19efe01324674c3ff0f06740d99

source rpm(s):

ftp://ftp.suse.com/pub/suse/x86_64/update/9.2/rpm/src/kernel-source-2.6.8-24.8.src.rpm
bc9e4a08ba429884716d9e1768ca7391
ftp://ftp.suse.com/pub/suse/x86_64/update/9.2/rpm/src/kernel-default-2.6.8-24.8.nosrc.rpm
0cbc4714154be7df7a18fda4c5ca595b

ftp://ftp.suse.com/pub/suse/x86_64/update/9.2/rpm/src/kernel-smp-2.6.8-24.8.nosrc.rpm
451d4c51a5d4083b4e663913bb53e622

ftp://ftp.suse.com/pub/suse/x86_64/update/9.2/rpm/src/kernel-default-2.6.8-24.8.nosrc.rpm
0cbc4714154be7df7a18fda4c5ca595b

ftp://ftp.suse.com/pub/suse/x86_64/update/9.2/rpm/src/kernel-smp-2.6.8-24.8.nosrc.rpm
451d4c51a5d4083b4e663913bb53e622

SUSE Linux 9.1:

ftp://ftp.suse.com/pub/suse/x86_64/update/9.1/rpm/x86_64/kernel-source-2.6.5-7.111.19.x86_64.rpm
9eaf681cb5ce3d0bca96dc93c2cbbe4d

ftp://ftp.suse.com/pub/suse/x86_64/update/9.1/rpm/x86_64/kernel-default-2.6.5-7.111.19.x86_64.rpm
1be1de01f36069168846ca611a9c493a

ftp://ftp.suse.com/pub/suse/x86_64/update/9.1/rpm/x86_64/kernel-smp-2.6.5-7.111.19.x86_64.rpm
905182441a3e0dfc19d241249f0bcd43

source rpm(s):

ftp://ftp.suse.com/pub/suse/x86_64/update/9.1/rpm/src/kernel-source-2.6.5-7.111.19.src.rpm
07caa57a7b036cc4e22f73744f0378f3

ftp://ftp.suse.com/pub/suse/x86_64/update/9.1/rpm/src/kernel-default-2.6.5-7.111.19.nosrc.rpm
15b023f310014e3327dde1a0bcf746c1

ftp://ftp.suse.com/pub/suse/x86_64/update/9.1/rpm/src/kernel-smp-2.6.5-7.111.19.nosrc.rpm
10c39d732cbafaeabb21f64aab518602

SUSE Linux 9.0:

ftp://ftp.suse.com/pub/suse/x86_64/update/9.0/rpm/x86_64/kernel-source-2.4.21-266.x86_64.rpm
981d7abbc9dd7774c724a3aec2508db1

ftp://ftp.suse.com/pub/suse/x86_64/update/9.0/rpm/x86_64/kernel-default-2.4.21-266.x86_64.rpm
47e4ec4f93d49abc0459a058526c1fb6

ftp://ftp.suse.com/pub/suse/x86_64/update/9.0/rpm/x86_64/kernel-smp-2.4.21-266.x86_64.rpm
03b0c0787d0a818634b11d4bbc533a38

ftp://ftp.suse.com/pub/suse/x86_64/update/9.0/rpm/x86_64/kernel-numa-2.4.21-149.x86_64.rpm
8877a1ca2ea3cb393aa96be727ca362e

source rpm(s):

ftp://ftp.suse.com/pub/suse/x86_64/update/9.0/rpm/src/kernel-source-2.4.21-266.src.rpm
326f9c08d5f92ccc3bca476977b745d6

ftp://ftp.suse.com/pub/suse/x86_64/update/9.0/rpm/src/kernel-default-2.4.21-266.src.rpm
ab01bf0aa3117ce642cc2eedebbba41b

ftp://ftp.suse.com/pub/suse/x86_64/update/9.0/rpm/src/kernel-smp-2.4.21-266.src.rpm
714b10cc3466776599cab8237223165f

ftp://ftp.suse.com/pub/suse/x86_64/update/9.0/rpm/src/kernel-numa-2.4.21-149.src.rpm
52c705df37ed9e44bb2943af318d8500

5) Pending vulnerabilities in SUSE Distributions and Workarounds:

Please see our Security Summary Report.

– problem with smbfs in the previous kernel update

We received reports of smbfs being broken by our last kernel update (released on Dec 1st, SUSE-SA:2004:042).

This apparently only affects the smbfs filesystem on 2.6 kernels, so SUSE Linux 9.1, 9.2, SUSE Linux Enterprise Server 9 and Novell Linux Desktop 9.

This problem is unfortunately not yet fixed in this security update, we will be releasing fixed packages in the begin of next year.

As workaround please change to use the cifs filesystem if possible, which replaces smbfs in the 2.6 kernel series.

6) standard appendix: authenticity verification, additional information

– Package authenticity verification:

SUSE update packages are available on many mirror ftp servers all over the world. While this service is being considered valuable and important to the free and open source software community, many users wish to be sure about the origin of the package and its content before installing the package. There are two verification methods that can be used independently from each other to prove the authenticity of a downloaded file or rpm package:

- 1) md5sums as provided in the (cryptographically signed) announcement.
- 2) using the internal gpg signatures of the rpm package.

1) execute the command

```
md5sum <name-of-the-file.rpm>
```

after you downloaded the file from a SUSE ftp server or its mirrors. Then, compare the resulting md5sum with the one that is listed in the announcement. Since the announcement containing the checksums is cryptographically signed (usually using the key security@suse.de), the checksums show proof of the authenticity of the package. We disrecommend to subscribe to security lists which cause the email message containing the announcement to be modified so that the signature does not match after transport through the mailing list software.

Downsides: You must be able to verify the authenticity of the announcement in the first place. If RPM packages are being rebuilt and a new version of a package is published on the ftp server, all md5 sums for the files are useless.

2) rpm package signatures provide an easy way to verify the authenticity of an rpm package. Use the command

```
rpm -v --checksig <file.rpm>
```

to verify the signature of the package, where <file.rpm> is the filename of the rpm package that you have downloaded. Of course, package authenticity verification can only target an un-installed rpm package file.

Prerequisites:

- a) gpg is installed
- b) The package is signed using a certain key. The public part of this key must be installed by the gpg program in the directory `~/.gnupg/` under the user's home directory who performs the signature verification (usually root). You can import the key that is used by SUSE in rpm packages for SUSE Linux by saving this announcement to a file ("announcement.txt") and running the command (do "su -" to be root):
`gpg --batch; gpg < announcement.txt | gpg --import`
SUSE Linux distributions version 7.1 and thereafter install the key "build@suse.de" upon installation or upgrade, provided that the package gpg is installed. The file containing the public key is placed at the top-level directory of the first CD (pubring.gpg) and at <ftp://ftp.suse.com/pub/suse/pubring.gpg-build.suse.de> .

– SUSE runs two security mailing lists to which any interested party may subscribe:

suse-security@suse.com

- general/linux/SUSE security discussion.
All SUSE security announcements are sent to this list.
To subscribe, send an email to
`<suse-security-subscribe@suse.com>`.

suse-security-announce@suse.com

- SUSE's announce-only mailing list.
Only SUSE's security announcements are sent to this list.
To subscribe, send an email to
`<suse-security-announce-subscribe@suse.com>`.

For general information or the frequently asked questions (FAQ) send mail to:

- `<suse-security-info@suse.com>` or
`<suse-security-faq@suse.com>` respectively.

=====

SUSE's security contact is `<security@suse.com>` or `<security@suse.de>`.
The `<security@suse.de>` public key is listed below.

=====

The information in this advisory may be distributed or reproduced, provided that the advisory is not modified in any way. In particular, it is desired that the clear-text signature shows proof of the authenticity of the text.

SUSE Linux AG makes no warranties of any kind whatsoever with respect to the information contained in this security advisory.

Type Bits/KeyID Date User ID
pub 2048R/3D25D3D9 1999-03-06 SuSE Security Team <security@suse.de>
pub 1024D/9C800ACA 2000-10-19 SuSE Package Signing Key <build@suse.de>

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: GnuPG v1.0.7 (GNU/Linux)

mQENAZbhLQQA AEIAK AkXHe0lWRBXLpn38hMHy03F0I4Sszmoc8aaKJrhfhyMIOA
BqvkIPL2f9UrI4Xc860gH79ZREwAgPt0pi6+SleNFLNcNFAuuHMLQOosAMFatbz
JR9i4m/lf6q929YROu5zB48rBAIcfTm+IBbijaEdnqpWgib45wE/Cfy6FAttBHQh
1Kp+r/jPbf1mYAvljUfHKuvbg8t2EIQz/5yGp+n5trn9pElfQO2cRBq8LFpf11+U
P7EKjFmlOq+Gs/fF98/dP3DfniSd78LQPq5vp8RL8nr/o2i7jkAQ33m4f1wOBWd+
cZovrKXYIXiR+Bf7m2hpZo+/sAzhd7LmAD0l09kABRG0JVN1U0UgU2VjdXJpdHkg
VGVhbSA8c2VjdXJpdHlAc3VzZS5kZT6JARUDBRA24S1H5Fiyh7HKPEUBAVcOB/9b
yHYji1/+4Xc2GhvXK0FSJN0MGgeXgW47yxDL7gmR4mNgjIIOUHJzj0PEpVjWepOJ7
tQS3L9oP6cpj1Fj/XxuLbkp5VCQ61hpt54coQAvYrnT9rtWEGN+xmweJT1WmYmDJ
xG+EGBXKr+XP69oIU1E2JO3rXekulgiqRKos4cdXKgyjWZ7CP9V9daRXdTje63
Om8gwSdU/nCvhdRIWp/Vwb7f7Ia8iZr9OJ5YuQl0DBG4qmGDDrvImgPAFkYFzwlqo
choXFQ9y0YVCV41DnR+GYhw12qBd81T8aXhihEGPIgaw3g8gd8B5o6mPVgl+nJqI
BkEYGBusiag2pS6qwznZiQEVAwUQNuEtBHey5gA9JdPZAQFtOaf+KVh939b0J94u
v/kpg4xs1LthlhqhbHcKNoVTNspugiC3qMPyvSX4XcBr2PC0cVks4Z9PY9iCfT+
x9WM96g39dAF+le2CCx7XISK9XXJ4ApEy5g4AuK7NYgAJd39PPBERgWnxjxir9g0
Ix30dS30bW39D+3NPU5Ho9TD/B7UDFvYt5AWHl3MGwo3a1RhTs6sfgL7yQ3U+mvq
MkTExZb5mfN1FeaYKMop0I4VpzNveGxQWlz67VjJHVyUIF20ekOz4kVWgsxkc8G2
saqZd6yv2EwqYTi8BDAduweP33KrQc4KDDommQND0XxaKOeCoESIdM4p7Esdjq1o
L0oixF12CohGBBARAgAGBQI7HmHDAoJEJ5A4xAACqukTIQAoI4QzP9yjPohY7OU
F7J3eKBTzp25AJ42BmtSd3pvm5ldmognWF3Trhp+GYkAlQMFEDe3O8IwkdF+zvyS
FQEBafkD/3GG5UgJj18UhYmh1gfjIIdcPAeqMwSytEHDENmHC+vLZQ/p0mT9tPiW
tp34io54mwr+bLPN8l6B5GJNkbGvH6M+m07R8Lj4nHL6pyAv3PQR83WyLHcaX7It
Klj371/4yzKV6qz43SGRK4MacLo2rNZ/dNej7lWPCtzCcFYwqkiiEYEEBECAAYF
AjoaQqQACgkQx1KqMrDf94ArewCfWnTUDG5gNYkmHG4bYL8fQcizyA4An2eVo/n+
3J2KRWSOhpAMsnMxtPbBiEYEEExECAAYFAkGJG+YACgkQGsiRhDTRlzm8CQCg14Wz
vg6j45e/r1oyt9EaHhleSacAnA+2dArk1I3xt49Z5rdnhqheF//9mQGIBDnu9IER
BACT8Y35+2vv4MGVKiLEMOI9GdSt6MckYS3yEKeueNWc+z/0Kvff4JctBsgs47tj
miI9sl0eHjm3gTR8rftXMN6sJEUHWzDP+Y0PFPboMvKx0FXl/A0dM+HFrruCGBlW
t6FA+okRySQiliuI5phwqkXefl9AhkwR8xocQSVCFxewwwCglVcOQliHu8jwRQHx
IRE0tkwQQI0D+wfQwKdvhDplxHJ5nf7U8c/yE/vdvpN6lF0tmFrKXBUX+K7u4ifr
ZlQvj/81M4InjtXreqDiJtr99Rs6xa0ScZqITuZC4CWxJa9GynBED3+D2t1V/f8l
0smsuYoFOF7Ib49IkTdbtwAThlZp8bEhELBeGaPdNCcmfZ66rKUdG5sRA/9ovnc1
krSQF2+sqB9/o7w5/q2qiyzwOSTnkjtBUVKn4zLUOf6aeBAoV6NMCC3Kj9aZhfA+
ND0ehPaVGJgjaVNFhPi4x0e7BULdvgOoAqajLfvkURHAeSsxXIoEmyW/xC1sBbDk
DUIBSx5oej73XCZgnj/inphRqGpsb+1nKFvF+rQoU3VTRSBQYWNrYWdlIFNpZ25p
bmcgS2V5IDxidWlsZEBzdXNlLmRlPohcBBMRagAcBQI57vSBBQkDwmcABAsKAwQD
FQMCAxYCAQIXgAAKCRCoTtronIAKy18sAJ98BgD40zw0GHJHIf6dNfnwI2PAsgCg
jH1+PnYEI7TFjtZsqhezX7vZvYCIRgQQEQIABgUCOnBeUgAKCRCEQOMQAAqrNzO
AKCL512FZvv4VZx94TpbA9lxyoAejACeO01HibActAevk5MUBhNeLZa/qM2JARUD
BRA6cGBvd7LmAD0l09kBATWnB/9An5vfiUUE1VQnt+T/EYkIES3tXXaJJp9pHMa4
fzFa8jPVtv5UBHGee3XoUNdVwM2OgSEISZxbzdXGnqIlcT08TzBUD9i579uifkL
snr35SJDZ6ram51/CWOnnaVhUzneOA9gTPSr+/ft3WeVnwJiQCQ30kNLVWXWATMn
snT486eAOIT6UNBPYQLpUprF5Yryk23pQUPAgJENDEqeU6iIO9Ot1ZPtB0lniw+/
xCi13D360o1tZDYOp0hHHJN3D3EN8C1yPqZd5CvvnYvB6bWBIPwCrgdn2DUVMmp
U661jwqGlrz1F84JG/xe4jGuzgpJt9IXSzyohEJB6XG5+D0BiF0EEExECAB0FAjxq
qTQFCQoAgrMFCwcKAwQDFQMCAxYCAQIXgAAKCRCoTtronIAKyp1fAJ9dR7saz2KP
NwD3U+fy/0BDKXrYgACfbJ8fQcJqCBQxeHvt9yMPDVq0B0W5Ag0EOe70khAIAISR
0E3ozF/la+oNaRwxHLrCet30NgnXRROyHPaJB/Tu1FQokn2/Qld/HZnh3TwhBIw1

FqrhWBJ7491iAjLR9uPbdWJrn+A7t8kSkPaF3Z/6kyc5a8fas44ht5h+6HMBzoFC
MAq2aBHQFRNp9Mz1ZvoXXcI1k118OqcUM/ovXbDfPcXsUveTPTtGzcAi2jV19h
l3iwJKkyv/RLmcusdsi8YunbvWGF5GaagYQo7YIF6UaBQnYJTM523AMgpPQtsK
m9o/w9WdgXkgWhghZEqUS3m5xNey1nLu9iMvq9M/iXnGz4sg6Q2Y+GqZ+yAvNW
jRRou3zSE7Bzg28MI4sAAwYH/2D71Xc5HPDgu87WnBFgmp8MpSr8QnSs0wwPg3xE
ullGEocolSb2c0ctuSyeVnCttJMzkukL9TqyF4s/6XRstWirSWawJxRLKH6Zjo/F
aKsshYKf8gBkAaddvpl3pO0gmUYbqmpQ3xDEYlhCeieXS5MkockQ1sj2xYdB1xO0
ExzfiCiscUKjUFy+mdzUsUutafuZ+gbHog1CN/ccZCkxcBa5IFCHORrNjq9pYWlr
xsEn6ApsG7JJbM2besW1PkdEoxak74z1senh36m5jQvVjA3U4xq1wwylxadmmJaJ
HzeiLfb7G1ZRjZTsB7fyYxqDzMVul6o9BSwO/1XsIAnV1uuITAQYEQIADAUCOe70
kgUJA8JnAAAKCRCoTtronIAKyksiAJsfB3/77SkH3JIYOGreE1O10JdGwACeKTtt
geVPFB+iGJdiwQlxasOfuXyITAQYEQIADAUCPGqpWQUJCgCCxwAKCRCoTtronIAK
yofBAKCSZM2UFyta/fe9WgITK9I5hbxxTQCfX+0ar2CZmSknn3coSPihn1+OBNw=
=Fv2n

-----END PGP PUBLIC KEY BLOCK-----

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.2.4 (GNU/Linux)

iQEVAwUBQch6Z3ey5gA9JdPZAQH3HQgAnuu2f4XzU4J5LhAWoUOsnBEARd6UJP3c
WCruYVbFFQHnEJylqwyJSrFLZ1/vWcVUIE6eEP5DDXmZqo4Yrbq/auNoZs7/35rZ
XJo7PPEVvPnyyvqH5a4Do0+mVkdHotxC6vltuEnryQO4X0ti5FVR7fOTLbBW/khW
QfbzoCTTS9yXA/mVTd3APZqsPpRdBdL3uLYBdkQ92+25TS+EKPRgo0xdvdxFaNsR
KmSMH1O+ki0xTRTrB//0WajHRS9WvyzrLhZJ8/pY1Q/4sWWwX/BJuXvTEscXDr15
QpLZFn5ASbhUV9qiPgQem8Bvx5zI1MwesE8BGUSvUWw8eAZGoH301g==
=BemR

-----END PGP SIGNATURE-----

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>