

SUSE Security Announcement: kernel various security and bugfixes (SUSE-SA:2005:068)

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2005-12/msg00184.html>

- *From:* Marcus Meissner <meissner@xxxxxxx>
 - *Date:* Wed, 14 Dec 2005 16:11:17 +0100
-

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

Hash: SHA1

SUSE Security Announcement

Package: kernel

Announcement ID: SUSE-SA:2005:068

Date: Wed, 14 Dec 2005 16:00:00 +0000

Affected Products: SUSE LINUX 9.3

SUSE LINUX 9.2

SUSE LINUX 9.1

SuSE Linux 9.0

SuSE Linux Desktop 1.0

SuSE Linux Enterprise Server 8

SUSE Linux Enterprise Server 9

UnitedLinux 1.0

Vulnerability Type: denial of service

Severity (1-10): 6

SUSE Default Package: yes

Cross-References: CVE-2005-1041, CVE-2005-2457, CVE-2005-2458

CVE-2005-2459, CVE-2005-2490, CVE-2005-2492

CVE-2005-2800, CVE-2005-2872, CVE-2005-2973

CVE-2005-3044, CVE-2005-3055, CVE-2005-3110

CVE-2005-3180, CVE-2005-3275, CVE-2005-3527

CVE-2005-3783, CVE-2005-3784, CVE-2005-3805

CVE-2005-3806, CVE-2005-3807

Content of This Advisory:

1) Security Vulnerability Resolved:

Linux kernel security problems and bugfixes

Problem Description

2) Solution or Work-Around

3) Special Instructions and Notes

4) Package Location and Checksums

5) Pending Vulnerabilities, Solutions, and Work-Arounds:

See SUSE Security Summary Report.

6) Authenticity Verification and Additional Information

1) Problem Description and Brief Discussion

The Linux kernel was updated to fix several security problems and several bugs, listed below:

Security fixes:

- CVE-2005-3783: A check in `ptrace(2)` handling that finds out if a process is attaching to itself was incorrect and could be used by a local attacker to crash the machine. (All)
- CVE-2005-3784: A check in reaping of terminating child processes did not consider `ptrace(2)` attached processes and would leave a `ptrace` reference dangling. This could lead to a local user being able to crash the machine. (Linux kernel 2.6 based products only)
- CVE-2005-2973: An infinite loop in the IPv6 UDP loopback handling can be easily triggered by a local user and lead to a denial of service. (Linux kernel 2.6 based products only)
- CVE-2005-3055: Unplugging an user space controlled USB device with an URB pending in user space could crash the kernel. This can be easily triggered by local attacker. (Fixed for Linux kernel 2.6 based products only.)
- CVE-2005-3044: Missing `sockfd_put()` calls in `routing_ioctl()` leaked file handles which in turn could exhaust system memory. (All)
- CVE-2005-3180: Fixed incorrect padding in Orinoco wireless driver, which could expose kernel data to the air. (Linux 2.6 based products only)
- CVE-2005-2490: A stack-based buffer overflow in the `sendmsg` function call in the Linux kernel 2.6 and 2.4 allowed local users execute arbitrary code by calling `sendmsg` and modifying the message contents in another thread. (All)
- CVE-2005-3806: A bug in IPv6 flow label handling code could be used by a local attacker to free non-allocated memory and in turn corrupt kernel memory and likely crash the machine. (All)
- CVE-2005-3275: The NAT code in Linux kernel incorrectly declares a variable to be static, which allows remote attackers to cause a denial of service (memory corruption) by causing two packets for the same protocol to be NATed at the same time. (All)
- CVE-2005-2457: A problem in decompression of files on "zisofs"

SUSE Security Announcement: kernel various security and bugfixes (SUSE-SA:2005:068)

filesystem was fixed. (All)

– CVE–2005–2458: A potential buffer overflow in the zlib decompression handling in the kernel was fixed. (All)

– CVE–2005–2459: Some return codes in zlib decoding were fixed which could have led to an attacker crashing the kernel. (All)

– CVE–2005–3110: A race condition in the ebtables netfilter module (ebtables.c), when running on an SMP system that is operating under a heavy load, might allow remote attackers to cause a denial of service (crash) via a series of packets that cause a value to be modified after it has been read but before it has been locked. (Linux kernel 2.6 based products only)

– CVE–2005–1041: A race condition when reading the /proc/net/route virtual file could be used by a local attacker to potentially crash the machine. (Linux kernel 2.6 based products only)

– CVE–2005–2800: A memory leak in the seq_file implementation in the SCSI procfs interface (sg.c) allows local users to cause a denial of service (memory consumption) via certain repeated reads from the /proc/scsi/sg/devices file, which is not properly handled when the next() iterator returns NULL or an error. (Linux kernel 2.6 based products only)

– CVE–2005–2872: The ipt_recent module when running on 64bit processors allows remote attackers to cause a DoS (kernel panic) via certain attacks such as SSH brute force. (Linux kernel 2.6 based products only)

– CVE–2005–2492: The raw_sendmsg function in the Linux kernel allows local attackers to cause a denial of service (change hardware state) or read from arbitrary memory via crafted input. (SUSE Linux 9.2 and 9.3)

– CVE–2005–3805: A locking problem in POSIX timer handling could be used by a local attacker on a SMP system to deadlock the machine. (SUSE Linux 9.3)

– CVE–2005–3527: A race condition in do_coredump in signal.c allows local users to cause a denial of service (machine hang) by triggering a core dump in one thread while another thread has a pending SIGSTOP. (SUSE Linux 9.3)

– CVE–2005–3807: A memory kernel leak in VFS lease handling can exhaust the machine memory and so cause a local denial of service. This is seen in regular Samba use and could also be triggered by local attackers. (SUSE Linux 9.3)

Non security bugfixes:

SUSE Security Announcement: kernel various security and bugfixes (SUSE-SA:2005:068)

- Fixed the "treason uncloaked" kernel messages that were caused by a stale `pred_flags` variable when the TCP `snd_wnd` changes.
- a lot of other small fixes not listed here.

2) Solution or Work-Around

There is no known workaround, please install the update packages.

3) Special Instructions and Notes

SPECIAL INSTALLATION INSTRUCTIONS

=====

The following paragraphs 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, make sure that you read through all of the steps below before attempting any of these procedures. All of the commands that need to be executed must be run as the superuser 'root'. Each step relies on the steps before it to complete successfully.

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

Use the following command to determine which kind of kernel is installed on your system:

```
rpm -qf --qf '%{name}\n' /boot/vmlinuz
```

**** Step 2: Download the packages for your system.

Download the kernel RPM package for your distribution with the name indicated by Step 1. Starting from SUSE LINUX 9.2, kernel modules that are not free were moved to a separate package with the suffix '-nongpl' in its name. Download that package as well if you rely on hardware that requires non-free drivers, such as some ISDN adapters. The list of all kernel RPM packages is appended below.

The kernel-source package does not contain a binary kernel in bootable form. Instead, it contains the sources that correspond with the binary kernel RPM packages. This package is required to build third party add-on modules.

**** Step 3: Verify authenticity of the packages.

Verify the authenticity of the kernel RPM package using the

methods as listed in Section 6 of this SUSE Security Announcement.

**** Step 4: Installing your kernel rpm package.

Install the rpm package that you have downloaded in Step 2 with the command

```
rpm -Uhv <FILE>
```

replacing <FILE> with the filename of the RPM package downloaded.

Warning: After performing this step, your system may not boot unless the following steps have been followed completely.

**** Step 5: Configuring and creating the initrd.

The initrd is a RAM disk that is loaded into the memory of your system together with the kernel boot image by the boot loader. The kernel uses the content of this RAM disk to execute commands that must be run before the kernel can mount its root file system. The initrd is typically used to load hard disk controller drivers and file system modules. The variable INITRD_MODULES in /etc/sysconfig/kernel determines which kernel modules are loaded in the initrd.

After a new kernel rpm has been installed, the initrd must be recreated to include the updated kernel modules. Usually this happens automatically when installing the kernel rpm. If creating the initrd fails for some reason, manually run the command

```
/sbin/mkinitrd
```

**** Step 6: Update the boot loader, if necessary.

Depending on your software configuration, you either have the LILO or GRUB boot loader installed and initialized on your system. Use the command

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

to find out which boot loader is configured.

The GRUB boot loader does not require any further action after a new kernel has been installed. You may proceed to the next step

if you are using GRUB.

If you use the LILO boot loader, lilo must be run to reinitialize the boot sector of the hard disk. Usually this happens automatically when installing the kernel RPM. In case this step fails, run the command

```
/sbin/lilo
```

Warning: An improperly installed boot loader will render your system unbootable.

**** Step 7: Reboot.

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

```
/sbin/shutdown -r now
```

Your system will now shut down and restart with the new kernel.

4) Package Location and Checksums

The preferred method for installing security updates is to use the YaST Online Update (YOU) tool. YOU detects which updates are required and automatically performs the necessary steps to verify and install them. Alternatively, download the update packages for your distribution manually and verify their integrity by the methods listed in Section 6 of this announcement. Then install the packages using the command

```
rpm -Fhv <file.rpm>
```

to apply the update, replacing <file.rpm> with the filename of the downloaded RPM package.

x86 Platform:

SUSE LINUX 9.3:

<ftp://ftp.suse.com/pub/suse/i386/update/9.3/rpm/i586/Intel-536ep-4.69-10.4.i586.rpm>
d500c2c08b8b7526d74023f65e59b85c

<ftp://ftp.suse.com/pub/suse/i386/update/9.3/rpm/i586/kernel-bigsmpl-2.6.11.4-21.10.i586.rpm>
6b7433eb3db4d6e0ee762966418e4dd9

<ftp://ftp.suse.com/pub/suse/i386/update/9.3/rpm/i586/kernel-bigsmpl-nongpl-2.6.11.4-21.10.i586.rpm>
c9915592a80dd81d26d7664887bf553d

<ftp://ftp.suse.com/pub/suse/i386/update/9.3/rpm/i586/kernel-default-2.6.11.4-21.10.i586.rpm>

SUSE Security Announcement: kernel various security and bugfixes (SUSE-SA:2005:068)

061bdddcee1a455b618990358fb6e9ed

<ftp://ftp.suse.com/pub/suse/i386/update/9.3/rpm/i586/kernel-default-nongpl-2.6.11.4-21.10.i586.rpm>
71109400fe245a1d9c927b51a886570c

<ftp://ftp.suse.com/pub/suse/i386/update/9.3/rpm/i586/kernel-smp-2.6.11.4-21.10.i586.rpm>
7814126834bc779f3b3f6c06ed2d9967

<ftp://ftp.suse.com/pub/suse/i386/update/9.3/rpm/i586/kernel-smp-nongpl-2.6.11.4-21.10.i586.rpm>
68ecf601f54b61f15df7ed7fb532816b

<ftp://ftp.suse.com/pub/suse/i386/update/9.3/rpm/i586/kernel-source-2.6.11.4-21.10.i586.rpm>
636f844e141e1f13d96ecc1fa1b0b083

<ftp://ftp.suse.com/pub/suse/i386/update/9.3/rpm/i586/kernel-syms-2.6.11.4-21.10.i586.rpm>
c68dea8979d7917a1d33d51ae5448c78

<ftp://ftp.suse.com/pub/suse/i386/update/9.3/rpm/i586/kernel-um-2.6.11.4-21.10.i586.rpm>
181375a1e7fb6ff0ac19f1eec1094df

<ftp://ftp.suse.com/pub/suse/i386/update/9.3/rpm/i586/kernel-um-nongpl-2.6.11.4-21.10.i586.rpm>
60d9c119d1754e7e722c20eebd1d8402

<ftp://ftp.suse.com/pub/suse/i386/update/9.3/rpm/i586/kernel-xen-2.6.11.4-21.10.i586.rpm>
188852e931d1f4ad7efc8ac35b258181

<ftp://ftp.suse.com/pub/suse/i386/update/9.3/rpm/i586/kernel-xen-nongpl-2.6.11.4-21.10.i586.rpm>
ce1e7f2365eec087c735921b5e6d9ccf

<ftp://ftp.suse.com/pub/suse/i386/update/9.3/rpm/i586/ltmodem-8.31a10-7.4.i586.rpm>
9fd2310063f308691a70d32e4f028549

<ftp://ftp.suse.com/pub/suse/i386/update/9.3/rpm/i586/um-host-install-initrd-1.0-50.4.i586.rpm>
bbedfc44ec6b5d44feaec1466171a6c5

<ftp://ftp.suse.com/pub/suse/i386/update/9.3/rpm/i586/um-host-kernel-2.6.11.4-21.10.i586.rpm>
2234c7a82681b61a75b5009f10ce47c7

SUSE LINUX 9.2:

<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/i586/Intel-536ep-4.69-5.12.i586.rpm>
8a47d92a848db8bdb55d6f0a6ab227de

<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/i586/kernel-bigsmpt-2.6.8-24.19.i586.rpm>
dace3bcedb831f4170055dc6f75cdabd

<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/i586/kernel-bigsmpt-nongpl-2.6.8-24.19.i586.rpm>
6e8c44794300272c7b285aac7f3454f0

<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/i586/kernel-default-2.6.8-24.19.i586.rpm>
61641b758f379ce5fb5c6d9b775860cb

<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/i586/kernel-default-nongpl-2.6.8-24.19.i586.rpm>
213170a1d5d872439f696d8489c4df8d

<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/i586/kernel-smp-2.6.8-24.19.i586.rpm>
75340371878caf30a19b0c0884e7c4b3

<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/i586/kernel-smp-nongpl-2.6.8-24.19.i586.rpm>
a319f80f554dc548f615258116c5eb82

<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/i586/kernel-source-2.6.8-24.19.i586.rpm>
f1307e25b9b03bd8bd31576a2dde93c8

<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/i586/kernel-syms-2.6.8-24.19.i586.rpm>
8ce4843272595ef052f3bcc106307c17

<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/i586/kernel-um-2.6.8-24.19.i586.rpm>
32c20befc06f9b5c6c21f675d7f27524

<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/i586/kernel-um-nongpl-2.6.8-24.19.i586.rpm>
c8e2e9d1f020f8e76cc5ca8df852e6e2

<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/i586/ltmodem-8.31a8-6.12.i586.rpm>
67170602966f4e3f948b5d247fe527c5

SUSE Security Announcement: kernel various security and bugfixes (SUSE-SA:2005:068)

<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/i586/um-host-install-initrd-1.0-48.11.i586.rpm>
5194a3b506192b7cea330c45f1015116

<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/i586/um-host-kernel-2.6.8-24.19.i586.rpm>
495f10410d45b5198a035afad1ab7060

SUSE LINUX 9.1:

<ftp://ftp.suse.com/pub/suse/i386/update/9.1/rpm/i586/kernel-bigsmpt-2.6.5-7.202.7.i586.rpm>
498b6452f6e80c2168fc18e9aaa171ca

<ftp://ftp.suse.com/pub/suse/i386/update/9.1/rpm/i586/kernel-default-2.6.5-7.202.7.i586.rpm>
9cdcc381aa3fe9c38883af5ae50fe566

<ftp://ftp.suse.com/pub/suse/i386/update/9.1/rpm/i586/kernel-smp-2.6.5-7.202.7.i586.rpm>
5b6910b080ddaebb52ba01a77e64cda5

<ftp://ftp.suse.com/pub/suse/i386/update/9.1/rpm/i586/kernel-source-2.6.5-7.202.7.i586.rpm>
f492f72cf5cc3039a02b0b809688ca49

<ftp://ftp.suse.com/pub/suse/i386/update/9.1/rpm/i586/kernel-syms-2.6.5-7.202.7.i586.rpm>
4613e41ca201515ae803966ecd7b0b93

<ftp://ftp.suse.com/pub/suse/i386/update/9.1/rpm/i586/ltmodem-2.6.2-38.19.i586.rpm>
d21af772ba56053116b350a1970777aa

SuSE Linux 9.0:

<ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/i586/Intel-536ep-4.62-27.i586.rpm>
df3caf24c8ece33169c54ff4672d373a

<ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/i586/Intel-v92ham-4.53-27.i586.rpm>
d0c7cfb40d369de915536fe376669731

ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/i586/k_athlon-2.4.21-303.i586.rpm
c85728e06562a696414f9bb6bc0441bc

ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/i586/k_deflt-2.4.21-303.i586.rpm
87d35dea039633533ce97976902adc24

ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/i586/k_smp-2.4.21-303.i586.rpm
313ed7c9eb5c96d5d60f31a72cef1b1c

ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/i586/k_smp4G-2.4.21-303.i586.rpm
d05c3ff5c412f82fb90434ad902ab076

ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/i586/k_um-2.4.21-303.i586.rpm
ea4422ee2da49a37626ab80c92c869a1

<ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/i586/kernel-source-2.4.21-303.i586.rpm>
8aa09607425053cc73fb11af0f08f107

<ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/i586/ltmodem-8.26a-216.i586.rpm>
39189597f72fd29c7bd95d25453a634c

Platform Independent:

SUSE LINUX 9.3:

<ftp://ftp.suse.com/pub/suse/i386/update/9.3/rpm/noarch/kernel-docs-2.6.11.4-21.10.noarch.rpm>
47d5b58910d7890c56b49c5f0a051edb

SUSE LINUX 9.2:

<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/noarch/kernel-docs-2.6.8-24.19.noarch.rpm>
d7d6524760444a7007b33614f7438d18

SUSE LINUX 9.1:

<ftp://ftp.suse.com/pub/suse/i386/update/9.1/rpm/noarch/kernel-docs-2.6.5-7.202.7.noarch.rpm>

SUSE Security Announcement: kernel various security and bugfixes (SUSE-SA:2005:068)

1c8fe8bd02541c36268c8bdd9ae52408

ftp://ftp.suse.com/pub/suse/x86_64/update/9.1/rpm/noarch/kernel-docs-2.6.5-7.202.7.noarch.rpm
4ccf9f952bf7bdf81535fae998ebcecf

x86-64 Platform:

SUSE LINUX 9.3:

ftp://ftp.suse.com/pub/suse/i386/update/9.3/rpm/x86_64/kernel-default-2.6.11.4-21.10.x86_64.rpm
ba425257f4863c3609218ffb97d88ad5

ftp://ftp.suse.com/pub/suse/i386/update/9.3/rpm/x86_64/kernel-default-nongpl-2.6.11.4-21.10.x86_64.rpm
4c5ce7b9a10a1befe1055e5dda1f8cf3

ftp://ftp.suse.com/pub/suse/i386/update/9.3/rpm/x86_64/kernel-smp-2.6.11.4-21.10.x86_64.rpm
3cbe380b73ab0582f272389241ed3387

ftp://ftp.suse.com/pub/suse/i386/update/9.3/rpm/x86_64/kernel-smp-nongpl-2.6.11.4-21.10.x86_64.rpm
4b42629c3bed66cacb1a984c5e26f9d4

ftp://ftp.suse.com/pub/suse/i386/update/9.3/rpm/x86_64/kernel-source-2.6.11.4-21.10.x86_64.rpm
06a6903d738d08d889486fd37fd356a8

ftp://ftp.suse.com/pub/suse/i386/update/9.3/rpm/x86_64/kernel-syms-2.6.11.4-21.10.x86_64.rpm
8e68e2009d0a7f75c844e66770d4c812

SUSE LINUX 9.2:

ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/x86_64/kernel-default-2.6.8-24.19.x86_64.rpm
205edc94cdc1efd47dcd5a3c207ed8ea

ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/x86_64/kernel-default-nongpl-2.6.8-24.19.x86_64.rpm
d165d199a24c2531ffb66bf8559f94d0

ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/x86_64/kernel-smp-2.6.8-24.19.x86_64.rpm
3741cd730f4d74fdd942df421dcd70c8

ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/x86_64/kernel-smp-nongpl-2.6.8-24.19.x86_64.rpm
a944dadclc00f35e0311cc1e059f2ef7

ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/x86_64/kernel-source-2.6.8-24.19.x86_64.rpm
10d243b42b080caf2b35a203d37e054b

ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/x86_64/kernel-syms-2.6.8-24.19.x86_64.rpm
476f6d22a5f9b985c6ff637b47560902

SUSE LINUX 9.1:

ftp://ftp.suse.com/pub/suse/x86_64/update/9.1/rpm/x86_64/kernel-default-2.6.5-7.202.7.x86_64.rpm
b842f83ea73c098b06264255c448a369

ftp://ftp.suse.com/pub/suse/x86_64/update/9.1/rpm/x86_64/kernel-smp-2.6.5-7.202.7.x86_64.rpm
67348b7d9c74d517652340c1b195d350

ftp://ftp.suse.com/pub/suse/x86_64/update/9.1/rpm/x86_64/kernel-source-2.6.5-7.202.7.x86_64.rpm
32a9ffb2b0907f4110ed577cc19f588e

ftp://ftp.suse.com/pub/suse/x86_64/update/9.1/rpm/x86_64/kernel-syms-2.6.5-7.202.7.x86_64.rpm
5f466140ede81eb3cf45a883c1a4283e

SuSE Linux 9.0:

ftp://ftp.suse.com/pub/suse/x86_64/update/9.0/rpm/x86_64/kernel-default-2.4.21-303.x86_64.rpm
995456b107b5a11541c441c01285c69f

ftp://ftp.suse.com/pub/suse/x86_64/update/9.0/rpm/x86_64/kernel-smp-2.4.21-303.x86_64.rpm
1330055b72a360e1e9d95f55446565c6

ftp://ftp.suse.com/pub/suse/x86_64/update/9.0/rpm/x86_64/kernel-source-2.4.21-303.x86_64.rpm
bfd3f18af242371f001ab3badb6886b6

SUSE Security Announcement: kernel various security and bugfixes (SUSE-SA:2005:068)

Sources:

SUSE LINUX 9.3:

<ftp://ftp.suse.com/pub/suse/i386/update/9.3/rpm/src/Intel-536ep-4.69-10.4.src.rpm>
f2864724ba6060f3eca93a52915f85d6
<ftp://ftp.suse.com/pub/suse/i386/update/9.3/rpm/src/kernel-bigsmpt-2.6.11.4-21.10.nosrc.rpm>
eb7b914b71b3a1a4714a40aeaf2fbcf9
<ftp://ftp.suse.com/pub/suse/i386/update/9.3/rpm/src/kernel-default-2.6.11.4-21.10.nosrc.rpm>
a747522cc3e547960f53cc56c7e8e25c
<ftp://ftp.suse.com/pub/suse/i386/update/9.3/rpm/src/kernel-docs-2.6.11.4-21.10.src.rpm>
33e9bdcde94a6aa836fdf2939b2c3595
<ftp://ftp.suse.com/pub/suse/i386/update/9.3/rpm/src/kernel-smp-2.6.11.4-21.10.nosrc.rpm>
d4b7a95149a614365f3c52a5536cb165
<ftp://ftp.suse.com/pub/suse/i386/update/9.3/rpm/src/kernel-source-2.6.11.4-21.10.src.rpm>
d3a5f22fed880743add67a900e010ab
<ftp://ftp.suse.com/pub/suse/i386/update/9.3/rpm/src/kernel-syms-2.6.11.4-21.10.src.rpm>
b76a34c01bf1da3ca175cfef88b62c47
<ftp://ftp.suse.com/pub/suse/i386/update/9.3/rpm/src/kernel-um-2.6.11.4-21.10.nosrc.rpm>
f5250e8c30889890e95f7ca39a5379b7
<ftp://ftp.suse.com/pub/suse/i386/update/9.3/rpm/src/kernel-xen-2.6.11.4-21.10.nosrc.rpm>
ea9714e45fafb92ac59de3e0ee10c1b2
<ftp://ftp.suse.com/pub/suse/i386/update/9.3/rpm/src/ltmodem-8.31a10-7.4.src.rpm>
fa31903dd77cab3c3f3f1e08bc288ae2
<ftp://ftp.suse.com/pub/suse/i386/update/9.3/rpm/src/um-host-install-initrd-1.0-50.4.src.rpm>
69bad0f07871a0e14bcfd6a5faba33d1

SUSE LINUX 9.2:

<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/src/Intel-536ep-4.69-5.12.src.rpm>
9cf828d9073188230d7d975eeb963e04
<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/src/kernel-bigsmpt-2.6.8-24.19.nosrc.rpm>
be8c729e22ca7e1e9a6ed5b7f833f84a
<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/src/kernel-default-2.6.8-24.19.nosrc.rpm>
bd66bc651a343c08045e22fe6156d416
<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/src/kernel-docs-2.6.8-24.19.src.rpm>
d83c27d1443592adfb6a5324c3fb2513
<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/src/kernel-smp-2.6.8-24.19.nosrc.rpm>
e9d751c304baba54601fb4be6f7cbe58
<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/src/kernel-source-2.6.8-24.19.src.rpm>
b7812ba431b9a0781268d022d70a9f6d
<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/src/kernel-syms-2.6.8-24.19.src.rpm>
ff9b86dd54d8ee09a06cb08505750c06
<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/src/kernel-um-2.6.8-24.19.nosrc.rpm>
46c82f4078918d1230299becee64a34a
<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/src/ltmodem-8.31a8-6.12.src.rpm>
22a1dc94736e4c1a401410d589eb69d8
<ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/src/um-host-install-initrd-1.0-48.11.src.rpm>
52621db970964619aa26e2c9cf9a9a8f

SUSE LINUX 9.1:

<ftp://ftp.suse.com/pub/suse/i386/update/9.1/rpm/src/kernel-bigsmpt-2.6.5-7.202.7.nosrc.rpm>

SUSE Security Announcement: kernel various security and bugfixes (SUSE-SA:2005:068)

00c430ebd996bee1e05479314963cb64

<ftp://ftp.suse.com/pub/suse/i386/update/9.1/rpm/src/kernel-default-2.6.5-7.202.7.nosrc.rpm>
665f6cd53c7cd95240cc78b1b3e47ac3

<ftp://ftp.suse.com/pub/suse/i386/update/9.1/rpm/src/kernel-docs-2.6.5-7.202.7.src.rpm>
89426852c558f249079da018691c3d78

<ftp://ftp.suse.com/pub/suse/i386/update/9.1/rpm/src/kernel-smp-2.6.5-7.202.7.nosrc.rpm>
9600effe6b950e0fd644381aadf33892

<ftp://ftp.suse.com/pub/suse/i386/update/9.1/rpm/src/kernel-source-2.6.5-7.202.7.src.rpm>
b81693fea5e535732ce38b6355f2039e

<ftp://ftp.suse.com/pub/suse/i386/update/9.1/rpm/src/kernel-syms-2.6.5-7.202.7.src.rpm>
6045f8cd31f5fadc64fc64f1a85a4dde

<ftp://ftp.suse.com/pub/suse/i386/update/9.1/rpm/src/ltmodem-2.6.2-38.19.src.rpm>
ca58518645ab07e0b15bca6d46fadab2

ftp://ftp.suse.com/pub/suse/x86_64/update/9.1/rpm/src/kernel-default-2.6.5-7.202.7.nosrc.rpm
bc4bf7caf9f40724fb6c8acbfabc83e

ftp://ftp.suse.com/pub/suse/x86_64/update/9.1/rpm/src/kernel-docs-2.6.5-7.202.7.src.rpm
d880cc8a4074451b58c837ad2ea89a62

ftp://ftp.suse.com/pub/suse/x86_64/update/9.1/rpm/src/kernel-smp-2.6.5-7.202.7.nosrc.rpm
91562eee5d7cd6bf85005525196a9ada

ftp://ftp.suse.com/pub/suse/x86_64/update/9.1/rpm/src/kernel-source-2.6.5-7.202.7.src.rpm
95b8fb67131984469558424c0311fe2c

ftp://ftp.suse.com/pub/suse/x86_64/update/9.1/rpm/src/kernel-syms-2.6.5-7.202.7.src.rpm
8cf7cb56943e24cc4dacaf61e03deef0

SuSE Linux 9.0:

<ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/src/Intel-536ep-4.62-27.src.rpm>
c8be7e60349bfd91c4fb380c7e5b6e2

<ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/src/Intel-v92ham-4.53-27.src.rpm>
dc26ab35f0c4c1de451a41e39d8477f0

ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/src/k_athlon-2.4.21-303.src.rpm
28603ac54a74a10f119b19dac4f70877

ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/src/k_deflt-2.4.21-303.src.rpm
bcd1ffba1492ca58fb972e762c92d55d

ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/src/k_smp-2.4.21-303.src.rpm
f8ef5667f2350a4dfa9d86ab1e75b71d

ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/src/k_smp4G-2.4.21-303.src.rpm
54a593469f9631cd3cdd82a01b49b81f

ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/src/k_um-2.4.21-303.src.rpm
2e116575b9de0e58e68fcc09a3c19f1

<ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/src/kernel-source-2.4.21-303.src.rpm>
992f6a2e95ec3d2c6c3b0d5a1f8e85c3

<ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/src/ltmodem-8.26a-216.src.rpm>
6870024817df87fdb801108bbee2d2d5

ftp://ftp.suse.com/pub/suse/x86_64/update/9.0/rpm/src/k_deflt-2.4.21-303.src.rpm
1a15fb38887d1f051594688ec17da243

ftp://ftp.suse.com/pub/suse/x86_64/update/9.0/rpm/src/k_smp-2.4.21-303.src.rpm
49ba0ba47e2dc4443ca5962fad818c5e

ftp://ftp.suse.com/pub/suse/x86_64/update/9.0/rpm/src/kernel-source-2.4.21-303.src.rpm
bb0660431c5fc18b52675b3394f63079

Our maintenance customers are notified individually. The packages are

SUSE Security Announcement: kernel various security and bugfixes (SUSE-SA:2005:068)

offered for installation from the maintenance web:

<http://support.novell.com/cgi-bin/search/searchtid.cgi?psdb/0efbd4214ff63cd671f6ac22674becbe.html>

<http://portal.suse.com/psdb/0efbd4214ff63cd671f6ac22674becbe.html>

<http://support.novell.com/cgi-bin/search/searchtid.cgi?psdb/20c5e4c2a0fea3202c966fa44c89b13e.html>

<http://portal.suse.com/psdb/20c5e4c2a0fea3202c966fa44c89b13e.html>

<http://support.novell.com/cgi-bin/search/searchtid.cgi?psdb/9fc2ed050cb64aa9c37f32a689e98703.html>

<http://portal.suse.com/psdb/9fc2ed050cb64aa9c37f32a689e98703.html>

<http://support.novell.com/cgi-bin/search/searchtid.cgi?psdb/79a129621653571f9f612232ddd69857.html>

<http://portal.suse.com/psdb/79a129621653571f9f612232ddd69857.html>

<http://support.novell.com/cgi-bin/search/searchtid.cgi?psdb/77fd150f1962b32355a96affeee048ed.html>

<http://portal.suse.com/psdb/77fd150f1962b32355a96affeee048ed.html>

<http://support.novell.com/cgi-bin/search/searchtid.cgi?psdb/93d7c163efacc0665439a7d2c93341d1.html>

<http://portal.suse.com/psdb/93d7c163efacc0665439a7d2c93341d1.html>

<http://support.novell.com/cgi-bin/search/searchtid.cgi?psdb/fcd8a24f5457e2ac521ea89935681fa3.html>

<http://portal.suse.com/psdb/fcd8a24f5457e2ac521ea89935681fa3.html>

<http://support.novell.com/cgi-bin/search/searchtid.cgi?psdb/c7050141b3702832a32e74185b621254.html>

<http://portal.suse.com/psdb/c7050141b3702832a32e74185b621254.html>

<http://support.novell.com/cgi-bin/search/searchtid.cgi?psdb/fa8599c9b2c6f42f6125cdf8246eb01.html>

<http://portal.suse.com/psdb/fa8599c9b2c6f42f6125cdf8246eb01.html>

<http://support.novell.com/cgi-bin/search/searchtid.cgi?psdb/f43a8157eaa3cc5d6ad4e782c86273d5.html>

<http://portal.suse.com/psdb/f43a8157eaa3cc5d6ad4e782c86273d5.html>

<http://support.novell.com/cgi-bin/search/searchtid.cgi?psdb/e400e6279f02255de204820f5290b8bb.html>

<http://portal.suse.com/psdb/e400e6279f02255de204820f5290b8bb.html>

<http://support.novell.com/cgi-bin/search/searchtid.cgi?psdb/268441775ca440ed04388897a55453d1.html>

<http://portal.suse.com/psdb/268441775ca440ed04388897a55453d1.html>

<http://support.novell.com/cgi-bin/search/searchtid.cgi?psdb/0e2c7f08437e0128f5441c08f313e453.html>

<http://portal.suse.com/psdb/0e2c7f08437e0128f5441c08f313e453.html>

5) Pending Vulnerabilities, Solutions, and Work-Arounds:

See SUSE Security Summary Report.

6) Authenticity Verification and Additional Information

– Announcement authenticity verification:

SUSE security announcements are published via mailing lists and on Web sites. The authenticity and integrity of a SUSE security announcement is guaranteed by a cryptographic signature in each announcement. All SUSE security announcements are published with a valid signature.

To verify the signature of the announcement, save it as text into a file and run the command

```
gpg --verify <file>
```

replacing <file> with the name of the file where you saved the announcement. The output for a valid signature looks like:

```
gpg: Signature made <DATE> using RSA key ID 3D25D3D9  
gpg: Good signature from "SuSE Security Team <security@xxxxxxx>"
```

where <DATE> is replaced by the date the document was signed.

If the security team's key is not contained in your key ring, you can import it from the first installation CD. To import the key, use the command

```
gpg --import gpg-pubkey-3d25d3d9-36e12d04.asc
```

– Package authenticity verification:

SUSE update packages are available on many mirror FTP servers all over the world. While this service is considered valuable and important to the free and open source software community, the authenticity and the integrity of a package needs to be verified to ensure that it has not been tampered with.

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) Using the internal gpg signatures of the rpm package
- 2) MD5 checksums as provided in this announcement

1) The internal 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, replacing <file.rpm> with the filename of the RPM package downloaded. The package is unmodified if it contains a valid signature from build@xxxxxxx with the key ID 9C800ACA.

This key is automatically imported into the RPM database (on RPMv4-based distributions) and the gpg key ring of 'root' during installation. You can also find it on the first installation CD and at

the end of this announcement.

2) If you need an alternative means of verification, use the md5sum command to verify the authenticity of the packages. Execute the command

```
md5sum <filename.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 SUSE security announcement. Because the announcement containing the checksums is cryptographically signed (by security@xxxxxxx), the checksums show proof of the authenticity of the package if the signature of the announcement is valid. Note that the md5 sums published in the SUSE Security Announcements are valid for the respective packages only. Newer versions of these packages cannot be verified.

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

suse-security@xxxxxxx

– General Linux and SUSE security discussion.

All SUSE security announcements are sent to this list.

To subscribe, send an e-mail to

<suse-security-subscribe@xxxxxxx>.

suse-security-announce@xxxxxxx

– SUSE's announce-only mailing list.

Only SUSE's security announcements are sent to this list.

To subscribe, send an e-mail to

<suse-security-announce-subscribe@xxxxxxx>.

For general information or the frequently asked questions (FAQ),

send mail to <suse-security-info@xxxxxxx> or

<suse-security-faq@xxxxxxx>.

=====

SUSE's security contact is <security@xxxxxxx> or <security@xxxxxxx>.

The <security@xxxxxxx> 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, the clear text signature should show proof of the authenticity of the text.

SUSE Linux Products GmbH provides 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@xxxxxxx>

SUSE Security Announcement: kernel various security and bugfixes (SUSE-SA:2005:068)

pub 1024D/9C800ACA 2000-10-19 SuSE Package Signing Key <build@xxxxxxx>

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

Version: GnuPG v1.0.6 (GNU/Linux)

Comment: For info see <http://www.gnupg.org>

mQGIBDnu9IERBACT8Y35+2vv4MGVKiLEMOI9GdST6MCKYS3yEKeueNWc+z/0Kvff
4JctBsgs47tjmiI9sl0eHjm3gTR8rItXMN6sJEUHWzDP+Y0PFPboMvKx0FXI/A0d
M+HFrruCGBIWt6FA+okRySQiliuI5phwqkXefl9AhkwR8xocQSVCFxcwvwCglVcO
QliHu8jwRQHxIRE0tkwQQI0D+wfQwKdvhDplxHJ5nf7U8c/yE/vdvpN6lF0tmFrK
XBUX+K7u4ifrZlQvj/81M4INjtXreqDiJtr99Rs6xa0ScZqITuZC4CWxJa9GynBE
D3+D2t1V/f8l0smsuYoFOF7Ib49IkTdbtwATHlZp8bEhELBeGaPdNCcmfZ66rKUD
G5sRA/9ovnc1krSQF2+sqB9/o7w5/q2qiyzwoSTnktBUVKn4zLUOf6aeBAoV6NM
CC3Kj9aZhfA+ND0ehPaVGJgjaVNFhPi4x0e7BULdvgOoAqajLfvkURHAeSsxXIoe
myW/xC1sBbDkDUIBSx5oej73XCZgnj/inphRqGpsb+1nKFvF+rQoU3VTRSBQYWNr
YWdlIFNpZ25pbmcgS2V5IDxidWlsZEBzdXNlMmRlPohcBBMRAgAcBQI57vSBBQkD
wmcABAsKAwQDFQMCAxYCAQIXgAAKCRCoTtronIAKyl8sAJ98BgD40zw0GHJHlf6d
NfnwI2PAsgCgjH1+PnYEI7TFjtZsqhezX7vZvYCIrGQQEQIABgUCOnBeUgAKCRCE
QOMQAAqrpNzOAKCL512FZvv4VZx94TpbA9lxyoAejACeOO1HIbActAevk5MUBhNe
LZa/qM2JARUDBRA6cGBvd7LmAD0I09kBATWnB/9An5vfiUUE1VQnt+T/EYkIES3t
XXaJp9pHMa4fzFa8jPVtv5UBHGee3XoUNdVwM2OgSEISZxbzdXGnqllcT08TzBU
D9i579uifkLsnr35SJDZ6ram51/CWOnnaVhUzneOA9gTPSr+/ft3WeVnwJiQCQ3
0kNLWVXWATMnsnT486eAOIT6UNBPYQLpUprF5Yryk23pQUPAgJENDEqeU6iO9Ot
1ZPtB0lniw+/xCi13D360o1tZDYOp0hHHJN3D3EN8C1yPqZd5CvvnZyVb6bWBIPW
cRgdn2DUVMmpU661jwqGIRz1F84JG/xe4jGuzgpJt9IXSzyohEJB6XG5+D0BiFOE
ExECAB0FAjxqqTQFCQoAgrMFCwcKAwQDFQMCAxYCAQIXgAAKCRCoTtronIAKyp1f
AJ9dR7saz2KPNwD3U+fy/0BDKXrYGACfbJ8fQcJqCBQxeHvt9yMPDVq0B0W5Ag0E
Oe70khAIAISR0E3ozF/la+oNaRwxHLrCet30NgnXRROYhPaJB/Tu1FQokn2/Qld/
HZnh3TwhBIw1FqrhWBJ7491iAjLR9uPbdWJrn+A7t8kSkPaF3Z/6kyc5a8fas44h
t5h+6HMBzoFCMAq2aBHQFRNp9Mz1ZvoXXc11k118OqcUM/ovXbDfPcXsUvETPT
tGzcAi2jVI9hl3iwJKkyv/RLmcusdsi8YunbvWGFaf5GaagYQo7YIF6UaBQnYJTM
523AMgppQtsKm9o/w9WdgXkgWhgkhZEEqUS3m5xNey1nLu9iMvq9M/iXnGz4sg6Q
2Y+GqZ+yAvNWjRRou3zSE7Bzg28MI4sAAwYH/2D71Xc5HPDgu87WnBFgmp8MpSr8
QnSs0wwPg3xEullGEocolSb2c0ctuSyeVnCttJMzkukL9TqyF4s/6XRstWirSWaw
JxRLKH6Zjo/FaKsshYKf8gBkAaddvpl3pO0gmUYbqmpQ3xDEYlhCeieXS5MkockQ
1sj2xYdB1xO0ExzfiCiscUKjUFy+mdzUsUutafuZ+gbHog1CN/ccZckxcBa5IFCH
ORrNjq9pYwlrxsEn6ApsG7JJbM2besW1PkdEoxak74z1senh36m5jQvVjA3U4xq1
wwylxadmJaJHzeiLfb7G1ZRjZTsB7fyYxqDzMVul6o9BSwO/1XsIAAnV1uuITAQY
EQIADAUCOe70kgUJA8JnAAAKCRCoTtronIAKysiaJsfB3/77SkH3JIYOGRee10I
0JdGwAcEKttgeVPFB+iGJdiwQlXasOfuXyITAQYEQIADAUCPGqpWQUJCgCCxwAK
CRCoTtronIAKyofBAKCSZM2UFyta/fe9WgITK9I5hbxtQCfX+0ar2CZmSknn3co
SPihnl+OBNyZAQ0DNuEtBAAAAQgAoCRcd7SVZEFcumffyEwflTcXQjhKzOahzxp
omuF+HIyU4AGq+SU8sTZ/1SsjhdzrSafv1IETACA+3SmLr5KV40Us1w0UC64cwt
A46xowVq1vMIH2Lib+V/qr3b1hE67nMHjysECVx9Ob4gFuKNoR2eqnAaJvJnAT8J
/LoUC20EdCHUqn6v+M9t/WZgC+WNR8cq69uDy3YQhDP/nlan6fm2uf2kSV9A7ZxE
GrwsWl/WX5Q/sQqMwaU6r4az98X3z90/cN+eJJ3vwtA+rm+nxEvyeV+jaLuOQBdf
ebh/XA4FZ35xmi+spdiVeJH4F/ubaGlmj7+wDOF3suYAPSXT2QAFebQIU3VTRSBT
ZWN1cml0eSBUZWFtIDxzZWN1cml0eUBzdXNlMmRlPohcBBMRAgAcBQI57vSBBQkD
RQEBVw4H/1vIdiOLX/7hdzYaG9crQVIk3QwaB5eBbjvLEMvuCZHiY2COUg5QdmPQ
8SIWNZ6k4nu1BLcv2g/pymPUWP9fG4tuSnIUDrWGM3nhyhAC9iudP2u1YQY37Gb
B6NPVaZiYMnEb4QYFcv5c/r2ghSXUTYk7etd6SW6WCOpEqizhx1cqDKNZnsI/X

```
11pFcO2N7rc6byDBJ1T+cK+F1Ehan9XBt/shryJmv04nli5CXQMEbiqYYMOu8iaA
8AWRgXPCWqhyGhcVD3LRhUJXjUOdH4ZiHCXaoF3zVPxpeGKEQY8iBrDeDyB3wHmj
qY9WCX6cmogGQRgYG6yJqDalLqrDOdmJARUDBRA24S0Ed7LmAD0109kBAW04B/4p
WH3f1vQn3i6/+SmDjGzUu2GwGq6Fsdwo2hVM2ym6CILeow/K9JfhdwGvY8LRxWRL
hn09j2IJ9P7H1Yz3qDf10AX6V7YILHtchKT1dcngCkTlMdgC4rs1iAA13f089sRG
BafGPGKv2DQjHfR1LfRtbf0P7c09Tkej1MP8HtQMW9hPkBYeXcwbCjdrVGFOzqx+
AvvJDdT6a+oyRMTFlvmZ83UV5pgoyimgjhWnM1V4bFBYjPrtWMkdXJSUXbR6Q7Pi
RZWCzGRzwbaxqpl3rK/YTCphOLwEMB27B4/fcqtBzgoMOiaZA0M5fFoo54KgRIh0
zinsSx2OrWgvSiLEXXYKiEYEEBECAAYFAjseYcMACgkQnkDjEAAKq6ROVACgjhDM
/3KM+iFjs5QXsnd4oFPonbkAnjYGa1J3em+bmV2aiCdYXdOuGn4ZiQCVAwUQN7c7
whaQN/7O/JIVAQEB+QP/cYblSAmPXxSFiaHWB+MiUNw8B6ozBLK0QcMQ2YcL6+VI
D+nSZP20+Ja2nfiKjnibCv5sss83yXoHkYk2Rsa8f0z6Y7tHwuPiccvqnIC/c9Cvz
dbIsdxpfsi0qWpFvX/jLmpXqqnPjdIZErgxpWujas1n9016PuXA8K3MJwVjCqSKI
RgQQEQIABgUCOhpCpAAKCRDHUqoysN/3gCt7AJ9adNQMbMA1iSYcbhtgvx9ByLPI
DgCfZ5Wj+f7cnYpFZI6GkAyyyczG09sE=
=LRKC
-----END PGP PUBLIC KEY BLOCK-----
```

```
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.2 (GNU/Linux)
```

```
iQEVAwUBQ6A1xney5gA9JdPZAQKD/Qf/VoLJnO1p+LMZH3RTNSPznwbip6OdlyVx
dZoSGnh+Y5Udn4ab0YR9iyPLE+vBj90dtU4pJXm9/cbZv+a4DjntnjMMMIJakAF
DNPPyNBtZi0OWNdUaYoOvfBC881x7e58mcq33FJgMYiyv38KSKdzAJkPFP18trwH
QQMB5s65BmFVXAkfFcgvZVsGq5WuRtuiZULdPlkm7CQk67JKWTUXmzfLVp1e0wuk
POEUubaq1zNjkCiW8TtA10Sg+tdtZKjHg9r5y+ITGbagz5kp2hySr57LtEKokcOI
b+DrSnLFscJaS0b/8NlnwJ/I7jk9iaQ6xFJqotn2FiNuVdyChDvemg==
=gbs9
-----END PGP SIGNATURE-----
```

-
- Prev by Date: [***RLA \("Remote LanD Attack"\)***](#)
 - Next by Date: [***CodeCon submission deadline reminder***](#)
 - Previous by thread: [***RLA \("Remote LanD Attack"\)***](#)
 - Next by thread: [***CodeCon submission deadline reminder***](#)
 - Index(es):
 - ◆ [***Date***](#)
 - ◆ [***Thread***](#)