

[Full-Disclosure] SUSE Security Announcement: Linux Kernel (SuSE-SA:2004:001)

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-01/0084.html>

From: Thomas Biege (*thomas_at_suse.de*)

Date: 01/05/04

To: full-disclosure@lists.netsys.com

Date: Mon, 5 Jan 2004 20:32:14 +0100 (CET)

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

SUSE Security Announcement

Package: Linux Kernel

Announcement-ID: SuSE-SA:2004:001

Date: Monday, Jan 5th 2004 20:27 MET

Affected products: 8.0, 8.1, 8.2, 9.0

SuSE Linux Enterprise Server 7,
SuSE Linux Database Server,
SuSE eMail Server III, 3.1
SuSE Linux Firewall on CD/Admin host
SuSE Linux Office Server
SuSE Linux Desktop 1.0
SuSE Linux School Server

Vulnerability Type: local system compromise

Severity (1-10): 6

SUSE default package: yes

Cross References:

Content of this advisory:

- 1) security vulnerability resolved:
 - incorrect bounds checkingproblem description, discussion, solution and upgrade information
- 2) pending vulnerabilities, solutions, workarounds:
 - mc
 - mod_gzip
 - tripwire
 - cvs
 - irssi
 - atftp
- 3) standard appendix (further information)

1) problem description, brief discussion, solution, upgrade information

The `do_mremap()` function of the Linux Kernel is used to manage (move, resize) Virtual Memory Areas (VMAs). By exploiting an incorrect bounds check in `do_mremap()` during the remapping of memory it is possible to create a VMA with the size of 0.

In normal operation `do_mremap()` leaves a memory hole of one page and creates an additional VMA of two pages. In case of exploitation no hole is created but the new VMA has a 0 bytes length.

The Linux Kernel's memory management is corrupted from this point and can be abused by local users to gain root privileges.

There is no temporary workaround for this bug.

Please note that on 8.1, the kernel-source package may not be installable through rpm, because of a bug in RPM (update of the kernel source RPM may take 30 minutes or more, or fail entirely). Owing to this problem, the kernel source is not available as a regular YOU update.

However, recognizing our obligation to publish the source along with the binary packages, we are making the source available as a compressed tar archive, downloadable from the normal FTP locations

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, you decide if the paragraph is needed for you or not. Please read through all of the steps down to the end. 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 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
```

The following options are possible (disregarding 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 chipsets  
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

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

Please download the kernel RPM package for your distribution with the name starting as indicated by Step 1. The list of all kernel rpm packages is appended below. Note: The kernel-source package does not contain any binary kernel in bootable form. Instead, it contains the sources that the binary kernel rpm packages are made 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 these locations below <ftp://ftp.suse.com/pub/suse/i386/update/>.

8.0/images/
8.1/rpm/i586
8.2/rpm/i586
9.0/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 applied.

If you run SUSE LINUX 8.1 and haven't applied the previous kernel update (SUSE-SA:2003:034), AND use 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 being 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 have a 7.x system, you must now run the command

```
lilo
```

as root to initialize the lilo bootloader for your system. Then proceed to the next step.

If you run a SUSE LINUX 8.x or a SLES8 system, there are two options: Depending on your software configuration, you have 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 applied to 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 are complete, then reboot using the command

```
shutdown -r now
```

or
init 6

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

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

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.

Missing packages will be published later.

Intel i386 Platform:

SuSE-9.0:

ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/i586/k_athlon-2.4.21-166.i586.rpm
0bbda4a9166edcdd4444fa43a5b37f10

source rpm(s):

ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/src/k_athlon-2.4.21-166.src.rpm
3cce21862c2d54a82742c74557dcc7fa

ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/i586/k_deflt-2.4.21-166.i586.rpm
6df247b9f114e8636de2c673747ef6ea

source rpm(s):

ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/src/k_deflt-2.4.21-166.src.rpm
c06a81d1e7912db429df25e8e8d754b7

ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/i586/k_smp-2.4.21-166.i586.rpm
0da9470eb573ecb5c801bedbd5dbf666

source rpm(s):

ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/src/k_smp-2.4.21-166.src.rpm
34393ea6b46a8b8859d51020e1dc275e

ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/i586/k_smp4G-2.4.21-166.i586.rpm
0b0d23a4a6918e57a1e7c45504a50df7

source rpm(s):

ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/src/k_smp4G-2.4.21-166.src.rpm
26cadc4c9d77dc6e433bedc458166236

ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/i586/k_um-2.4.21-166.i586.rpm
7e18d9b0b89ef72bee40bbf150dd0470

source rpm(s):

ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/src/k_um-2.4.21-166.src.rpm
ad8c357792c0d34570c9ba54a579d867

<ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/i586/kernel-source-2.4.21-166.i586.rpm>
48b46c943cc15aacfba0ec68090de1f6

source rpm(s):

<ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/src/kernel-source-2.4.21-166.src.rpm>
ef71c55f61b595edc24be7c318237432

SuSE-8.2:

ftp://ftp.suse.com/pub/suse/i386/update/8.2/rpm/i586/k_athlon-2.4.20-102.i586.rpm
61de636fab3149ee5d45d16dccf8d0e8

source rpm(s):

ftp://ftp.suse.com/pub/suse/i386/update/8.2/rpm/src/k_athlon-2.4.20-102.src.rpm
80b8f44b6f8f4d039b8954c709b457b0

ftp://ftp.suse.com/pub/suse/i386/update/8.2/rpm/i586/k_deflt-2.4.20-102.i586.rpm
c25b57bc5d67d87177abf7953f022331

source rpm(s):

ftp://ftp.suse.com/pub/suse/i386/update/8.2/rpm/src/k_deflt-2.4.20-102.src.rpm
29d014e79a3ee0b14a23cb0e4bdd0f0e

ftp://ftp.suse.com/pub/suse/i386/update/8.2/rpm/i586/k_smp-2.4.20-102.i586.rpm
d42041b08cdee2d9959a4a6dad8b6e9d

source rpm(s):

ftp://ftp.suse.com/pub/suse/i386/update/8.2/rpm/src/k_smp-2.4.20-102.src.rpm
22e598ebf546cd9378c852042b602f2f

ftp://ftp.suse.com/pub/suse/i386/update/8.2/rpm/i586/k_psmp-2.4.20-102.i586.rpm
c2e0455b45eac55c97e13322ab40e4bc

source rpm(s):

ftp://ftp.suse.com/pub/suse/i386/update/8.2/rpm/src/k_psmp-2.4.20-102.src.rpm
68b2d35ae0de009ac3fbc6ee9a0bb3fd

<ftp://ftp.suse.com/pub/suse/i386/update/8.2/rpm/i586/kernel-source-2.4.20.SuSE-102.i586.rpm>
0f539af39523fd27232289014db36202

source rpm(s):

<ftp://ftp.suse.com/pub/suse/i386/update/8.2/rpm/src/kernel-source-2.4.20.SuSE-102.src.rpm>
14c238bbbd7758abc2b4113a7297f2b5

SuSE-8.1:

ftp://ftp.suse.com/pub/suse/i386/update/8.1/rpm/i586/k_athlon-2.4.21-168.i586.rpm
8299b1153d3d9d81236e4e77f3ae66e2

source rpm(s):

ftp://ftp.suse.com/pub/suse/i386/update/8.1/rpm/src/k_athlon-2.4.21-168.src.rpm
0705e6bb739aaec77bc9801760e60051

ftp://ftp.suse.com/pub/suse/i386/update/8.1/rpm/i586/k_deflt-2.4.21-168.i586.rpm
fea1ffe95acdbc5c00d3272b3867bd39

source rpm(s):

ftp://ftp.suse.com/pub/suse/i386/update/8.1/rpm/src/k_deflt-2.4.21-168.src.rpm
aef9339c71c275fd3c7e9ebcf49cc4f

ftp://ftp.suse.com/pub/suse/i386/update/8.1/rpm/i586/k_smp-2.4.21-168.i586.rpm
f4e41bdd0806673d82dc0971e36da0e1

source rpm(s):

ftp://ftp.suse.com/pub/suse/i386/update/8.1/rpm/src/k_smp-2.4.21-168.src.rpm
f352afbf4c6d679fd4bf40347bd7989c

ftp://ftp.suse.com/pub/suse/i386/update/8.1/rpm/i586/k_debug-2.4.21-168.i586.rpm
81e9a2516e7b9a8d0234f2d6ee9e4444

source rpm(s):

ftp://ftp.suse.com/pub/suse/i386/update/8.1/rpm/src/k_debug-2.4.21-168.src.rpm
8b6c8e51c93c9dcbf5d34587de722a4a

ftp://ftp.suse.com/pub/suse/i386/update/8.1/rpm/i586/k_psmp-2.4.21-168.i586.rpm
9961f14d44c40a83be800ad463e17e51

source rpm(s):

Full-Disclosure: [Full-Disclosure] SUSE Security Announcement: Linux Kernel (SuSE-SA:2004:001)

ftp://ftp.suse.com/pub/suse/i386/update/8.1/rpm/src/k_psmpt-2.4.21-168.src.rpm
f3caa2e715d24a2987408e29e0623737

SuSE-8.0:

ftp://ftp.suse.com/pub/suse/i386/update/8.0/images/k_deflt-2.4.18-282.i386.rpm
62ae55de1c6abbe821b99165cbccdce7

source rpm(s):

ftp://ftp.suse.com/pub/suse/i386/update/8.0/zq1/k_deflt-2.4.18-282.src.rpm
c65eadb1dd7225463f7a29979ab43dd8

ftp://ftp.suse.com/pub/suse/i386/update/8.0/images/k_smp-2.4.18-282.i386.rpm
7fdec3995171a6d88f293c10c41e6991

source rpm(s):

ftp://ftp.suse.com/pub/suse/i386/update/8.0/zq1/k_smp-2.4.18-282.src.rpm
08a2cba4382f4bb8adfc5cb8f80677d1

ftp://ftp.suse.com/pub/suse/i386/update/8.0/images/k_psmpt-2.4.18-282.i386.rpm
955386318df968aac6c66b6071eb466a

source rpm(s):

ftp://ftp.suse.com/pub/suse/i386/update/8.0/zq1/k_psmpt-2.4.18-282.src.rpm
fe87f59c3e818fbb9eedcb211f9d0bf4

<ftp://ftp.suse.com/pub/suse/i386/update/8.0/d3/kernel-source-2.4.18.SuSE-282.i386.rpm>
249a3cd1dcc1edaabf00d72874ba4aa2

source rpm(s):

<ftp://ftp.suse.com/pub/suse/i386/update/8.0/zq1/kernel-source-2.4.18.SuSE-282.nosrc.rpm>
7e5cbc3af87fdebd8b6dc829e038d63

ftp://ftp.suse.com/pub/suse/i386/update/8.0/images/k_i386-2.4.18-282.i386.rpm
bd80346beef2e459009584065fcc7eb

source rpm(s):

ftp://ftp.suse.com/pub/suse/i386/update/8.0/zq1/k_i386-2.4.18-282.src.rpm
ce704a3481d8b84f9fdd0b83784e74a6

Opteron x86_64 Platform:

SuSE-9.0:

ftp://ftp.suse.com/pub/suse/x86_64/update/9.0/rpm/x86_64/k_deflt-2.4.21-171.x86_64.rpm
3dd54a4105bad6c4f3084e70aaa45410

source rpm(s):

ftp://ftp.suse.com/pub/suse/x86_64/update/9.0/rpm/src/k_deflt-2.4.21-171.src.rpm
d88ca0142409a98a7e4e9f4f7b2e9bf8

ftp://ftp.suse.com/pub/suse/x86_64/update/9.0/rpm/x86_64/k_smp-2.4.21-171.x86_64.rpm
b97e9d91ef710b0b801536294d99ba1a

source rpm(s):

ftp://ftp.suse.com/pub/suse/x86_64/update/9.0/rpm/src/k_smp-2.4.21-171.src.rpm
6221b0f5893499f5926c9dd529fceb5c

ftp://ftp.suse.com/pub/suse/x86_64/update/9.0/rpm/x86_64/kernel-source-2.4.21-171.x86_64.rpm
1a27668dff4ae3c405f18399432a326e

source rpm(s):

ftp://ftp.suse.com/pub/suse/x86_64/update/9.0/rpm/src/kernel-source-2.4.21-171.src.rpm
301e1d8ac232d3a000f373a928deee5f

2) Pending vulnerabilities in SUSE Distributions and Workarounds:

– mc

By using a special combination of links in archive-files it is possible to execute arbitrary commands while mc tries to open it in its VFS. The packages will be release as soon.

– mod_gzip

The apache module mod_gzip is vulnerable to remote code execution while running in debug-mode. We do not ship this module in debug-mode but future versions will include the fix.

Additionally the mod_gzip code was audited to fix more possible security related bugs.

– tripwire

Tripwire is a file integrity checker. The tripwire version on SuSE Linux 8.2 and 9.0 do crash when a requested file does not exists.

New packages will be available soon.

– cvs

The cvs server-side can be tricked to create files in the root filesystem of the server by requesting malformed modules. The permissions on the root filesystem normally prevent this malfunction.

New packages will be available soon.

– irssi

Under special circumstances the the irc-client irssi can be crashed remotely by other irc-clients.

New packages are available on our FTP servers.

– atftp

A buffer overflow vulnerability discovered by Rick Patel has been fixed in the atftpd (trivial file transfer protocol, UDP oriented) daemon, contained in the atftp package. Update packages for the affected SUSE Linux distributions 8.1 and 8.2 have been published on our ftp server today.

We explicitly thank Dirk Mueller, KDE developer, for notifying SUSE Security about the pending treatment of this incident.

New packages are available on our FTP servers.

3) 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 v1.0.6 (GNU/Linux)

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

mQGIBDnu9IERBACT8Y35+2vv4MGVkiLEMOI9GdST6MCKYS3yEKeueNWc+z/0Kvff
4JctBsgs47tjmiI9sl0eHjm3gTR8rItXMN6sJEUHWzDP+Y0PFPboMvKx0FXl/A0d
M+HFrruCGBIWt6FA+okRySQiliuI5phwqkXefl9AhkwR8xocQSVCFxcwvwcglVcO
QliHu8jwRQHxlRE0tkwQQI0D+wfQwKdvhDplxHJ5nf7U8c/yE/vdvpN6lF0tmFrK
XBUX+K7u4ifrzlQvj/81M4INjtXreqDiJtr99Rs6xa0ScZqITuZC4CWxJa9GynBE
D3+D2t1V/f8l0smsuYoFOF7Ib49IkTdbtwAThlZp8bEhELBeGaPdNCcmfZ66rKUd
G5sRA/9ovnc1krSQF2+sqB9/o7w5/q2qiyzwOSTnkjtBUVKn4zLUOf6aeBAoV6NM
CC3Kj9aZhfA+ND0ehPaVGJgjaVNFhPi4x0e7BULdvgOoAqajLfvkURHAeSsxXIoe
myW/xC1sBbDkDUIBSx5oej73XCZgnj/inphRqGpsb+InKFvF+rQoU3VTRSBQYWNr
YWdlIFNpZ25pbmcgS2V5IDxidWlsZEBzdXNlMlRlPohcBBMRAgAcBQI57vSBBQkD
wmcABAsKAwQDFQMCAxYCAQIXgAAKCRCoTtronIAKy18sAJ98BgD40zw0GHJHif6d
NfnwI2PAsgCgjH1+PnYEI7TFjtZsqhezX7vZvYCIRgQQEQIABgUCOnBeUgAKCRce
QOMQAAqrpNzOAKCL512FZvv4VZx94TpbA9lxyoAejACeOO1HIbActAevk5MUBhNe
LZa/qM2JARUDBRA6cGBvd7LmAD0l09kBATWnB/9An5vfiUUE1VQnt+T/EYkIES3t
XXaJp9pHMa4fzFa8jPvtv5UBHGee3XoUNdVwM2OgSEISZxbzdXGnqllcT08TzBU
D9i579uifklLsnr35SJDZ6ram51/CWOnnaVhUzneOA9gTPSr+/ft3WeVnwJiQCQ3
0kNLWVXWATMnsnT486eAOIT6UNBPYQLpUprF5Yryk23pQUPAgJENDeqeU6iIO9Ot

1ZPtB0lniw+/xCi13D360o1tZDYOp0hHHJN3D3EN8C1yPqZd5CvvnYvB6bWBIPw
cRgdn2DUVMmpU661jwqGIRz1F84JG/xe4jGuzgpJt9IXSzyohEJB6XG5+D0BiFOE
ExECAB0FAjxqqTQFCQoAgrMFCwcKAwQDFQMCaxYCAQIXgAAKCRCoTtronIAKyp1f
AJ9dR7saz2KPNwD3U+fy/0BDKXrYGACfbJ8fQcJqCBQxeHvt9yMPDVq0B0W5Ag0E
Oe70khAIAISR0E3ozF/la+oNaRwxHLrCet30NgnxRROYhPaJB/Tu1FQokn2/Qld/
HZnh3TwhBIw1FqrhWBJ7491iAjLR9uPbdWJrn+A7t8kSkPaF3Z/6kyc5a8fas44h
t5h+6HMBzoFCMAq2aBHQRFrNp9Mz1ZvoXXc11k118OqcUM/ovXbDfPcXsUVeTPT
tGzcAi2jVI9h3iwJKkyv/RLmcusdsi8YunbvWGFAF5GaagYQo7YIF6UaBQnYJTM
523AMgpPQtsKm9o/w9WdgXkgWhgkhZEEqUS3m5xNey1nLu9iMvq9M/iXnGz4sg6Q
2Y+GqZ+yAvNWjRRou3zSE7Bzg28MI4sAAwYH/2D71Xc5HPDgu87WnBFgmp8MpSr8
QnSs0wwPg3xEullGEocolSb2c0ctuSyeVnCttJMzkukL9TqyF4s/6XRstWirSWaw
JxRLKH6Zjo/FaKsshYKf8gBkAaddvpl3pO0gmUYbqmpQ3xDEYlhCeieXS5MkockQ
1sj2xYdB1xO0ExzfiCiscUKjUFy+mdzUsUutafuZ+gbHog1CN/ccZCkxcBa5IFCH
ORrNjq9pYwlrXsEn6ApsG7JJbM2besW1PkdEoxak74z1senh36m5jQvVjA3U4xq1
wwylxadmmJaJHzeiLfb7G1ZRjZTsB7fyYxqDzMVul6o9BSwO/1XsIANV1uuITAQY
EQIADAUCOe70kgUJA8JnAAAKCRCoTtronIAKysiaJsfB3/77SkH3JIYOGREe1Ol
0JdGwAcEKtTtgeVPFB+iGJdiwQlxasOfuXyITAQYEQIADAUCPGqpWQUJCgCCxwAK
CRCoTtronIAKyoFBAKCSZM2UFyta/fe9WgITK9I5hbxxTQCfX+0ar2CZmSknn3co
SPihnl+OBNyZAQ0DNuEtBAAAAQgAoCRcd7SVZEFcumffyEwflTcXQjhKzOahzxp
omuF+HlyU4AGq+SU8sTZ/1SsjhdzrSAfv1IETACA+3SmLr5KV40Us1w0UC64cwt
A46xowVq1vMIH2Lib+V/qR3b1hE67nMHjysECVx9Ob4gFuKNoR2eqnAaJvjaAT8J
/LoUC20EdCHUqn6v+M9t/WZgC+WNR8cq69uDy3YQhDP/nIanf6m2uf2kSV9A7Zx
EGrwsWl/WX5Q/sQqMwaU6r4az98X3z90/cN+eJJ3vwtA+rm+nxEvyeV+jaLuOQBdf
ebh/XA4FZ35xmi+spdiVeJH4F/ubaGlmj7+wDOF3suYAPSXT2QAFebQIU3VTRSBT
ZWN1cml0eSBUZWFtIDxzZWN1cml0eUBzdXNlMlRlPpOkBFQMFEDbhLUfkWLKHsco8
RQEBVw4H/1vIdiOLX/7hdzYaG9crQVik3QwaB5eBbjvLEMvuCZHiY2COUg5QdmPQ
8SIWNZ6k4nu1BLcv2g/pymPUWP9fG4tuSnIUDrWGm3nhyhAC9iudP2u1YQY37Gb
B6NPVaZiYmNEb4QYFcv5c/r2ghSXUTYk7etd6SW6WCOPEqizhx1cqDKNZnsI/1X
11pFc02N7rc6byDBJ1T+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+V1
D+nSZP20+Ja2nfiKjnibCv5ss83yXoHkYk2Rsa8foz6Y7tHwuPiccvqnlC/c9Cvz
dbIsdxpfsi0qWPfvX/jLMpXqqnPjdIZErgxpWujas1n9016PuXA8K3MJwVjCqSKI
RgQQEQIABgUCOhpCpAAKCRDHUqoysN/3gCt7AJ9adNQMbmA1iSYcbhtgvx9ByLPI
DgCfZ5Wj+f7cnYpFZI6GkAayczG09sE=
=LRKC

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

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

Version: GnuPG v1.0.7 (GNU/Linux)

iQEVAwUBP/m68Xey5gA9JdPZAQGZRAf/fLimM8z4Cw2pAJM1hev5vLJeEoLeztzm
PmSjfn4XqybiMeJf2u+40i4GwDkYdHk5kcl7Hr/1bt1t2IKD6XCY7rYGeXLcXRv

Full-Disclosure: [Full-Disclosure] SUSE Security Announcement: Linux Kernel (SuSE-SA:2004:001)

E2+AAwvdYO+U7qvSGkyxDU+ukNAESR1FV9kVftaPm7PcML99cWHrIJnboKtVhMD6
CNV3TeGpoRTzjZMpL4E34wPj28LpVzqbH7dX2wDPRVzggkWrV2+hnE3UA4q9tO5D
yvtBLzhQXR9dChb9oLKKZdABpDdeWThdftsgHgPz5Q+Ct5fPUheUqos0Xplgx6te
LU/RZcLX9YDLe8HdJ1FiHvHHMFRQsatwTXcvHUSNbUC6b6PwD2nTaA==
=xrmT
-----END PGP SIGNATURE-----

Full-Disclosure – We believe in it.

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