

Mail server administrators should seriously consider upgrading their servers (Linux Reviews)

> [Linux Reviews](#) > [News and headlines](#) > [2005 News archive](#) > [March](#) >

# Mail server administrators should seriously consider upgrading their servers

*LinuxReviews.org*

Security problems were found in the mail packages UW-Imap and cyrus-imapd the last week.

---

1. [UW-IMAP, Suse announcement](#)
  2. [Cyrus-imapd, Suse announcement](#)
- 

Security vulnerabilities are found in the University of Washington IMAP (UW-IMAP) server. Updated packages are now available for [GENTOO](#), [MANDRAKE](#), [REDHAT](#) and [SUSE](#). The problem is assigned [CAN-2005-0198](#).

A similar problem was found in the Cyrus-Imap server last week, updated packages for Cyrus-Imap are also available for these distributions.

It is also a generally good idea to [upgrade curl](#) while you are at it.

## 1. UW-IMAP, Suse announcement

...

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

---

### SUSE Security Announcement

Package: imap  
Announcement-ID: SUSE-SA:2005:012  
Date: Tue, 1 Mar 2005 10:00:00 +0000  
Affected products: 8.2, 9.0, 9.1, 9.2  
SUSE Linux Enterprise Server 8, 9  
Vulnerability Type: remote authentication bypass  
Severity (1-10): 6  
SUSE default package: no  
Cross References: CAN-2005-0198

Content of this advisory:

- 1) security vulnerability resolved:  
CRAM-MD5 authentication bug  
problem description
- 2) solution/workaround
- 3) special instructions and notes
- 4) package location and checksums
- 5) pending vulnerabilities, solutions, workarounds:  
See SUSE Security Summary Report.
- 6) standard appendix (further information)

## Mail server administrators should seriously consider upgrading their servers (Linux Reviews)

---

### 1) problem description, brief discussion

The University of Washington imap daemon can be used to access mails remotely using the IMAP protocol.

This update fixes a logical error in the challenge response authentication mechanism CRAM-MD5 used by UW IMAP. Due to this mistake a remote attacker can gain access to the IMAP server as arbitrary user.

This is tracked by the Mitre CVE ID CAN-2005-0198.

### 2) solution/workaround

None, please install the updated packages.

### 3) special instructions and notes

None.

### 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/imap-2004a-3.2.i586.rpm  
2b4cf0f70fb0164a90f6e73b66f28c5a

SUSE Linux 9.1:

ftp://ftp.suse.com/pub/suse/i386/update/9.1/rpm/i586/imap-2002e-92.4.i586.rpm  
32eb45928cf31bb0cbae78139303561b

SUSE Linux 9.0:

ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/i586/imap-2002d-59.i586.rpm  
b8af4a9008cb1d311f650700b6d642c5

SUSE Linux 8.2:

ftp://ftp.suse.com/pub/suse/i386/update/8.2/rpm/i586/imap-2002-56.i586.rpm  
6f73b1197b2a095fc30b8afde860f5fe

x86-64 Platform:

SUSE Linux 9.2:

ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/x86\_64/imap-2004a-3.2.x86\_64.rpm  
a6a79a3e1459dd1d5799e40257684d4e

source rpm(s):

ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/src/imap-2004a-3.2.src.rpm  
18201a6f78b73d2250f6ea0e614049b2

SUSE Linux 9.1:

ftp://ftp.suse.com/pub/suse/x86\_64/update/9.1/rpm/x86\_64/imap-2002e-92.4.x86\_64.rpm

## Mail server administrators should seriously consider upgrading their servers (Linux Reviews)

```
007c9777aacc36dec72067cf6ac39e7d
source rpm(s):
ftp://ftp.suse.com/pub/suse/x86_64/update/9.1/rpm/src/imap-2002e-92.4.src.rpm
    9bf8dda300636e712f164d784bc131a5

SUSE Linux 9.0:
ftp://ftp.suse.com/pub/suse/x86_64/update/9.0/rpm/x86_64/imap-2002d-59.x86_64.rpm
    25ffa1aa178c962753bc26483d0e9354
source rpm(s):
ftp://ftp.suse.com/pub/suse/x86_64/update/9.0/rpm/src/imap-2002d-59.src.rpm
    2da3ea9899a1ddf909d7dc5059138e7d
```

---

### 5) Pending vulnerabilities in SUSE Distributions and Workarounds:

See SUSE Security Summary Report.

---

### 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

## Mail server administrators should seriously consider upgrading their servers (Linux Reviews)

~/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>.  
<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+2vv4MGVKiLEMO19GdST6MCKYS3yEKeueNWc+z/0Kvff
4JctBsgs47tjmiI9s10eHjm3gTR8rItXMN6sJEUHWzDP+Y0PFpboMvKx0FX1/A0d
M+HFrruCGBlWt6FA+okRySQilIuI5phwqkXefl9AhkWR8xocQSVCFxcwvvcg1VcO
QliHu8jwRQHx1RE0tkwQOI0D+wFQwKdvhDplxHJ5nf7U8c/yE/vdvpN61F0tmFrK
XBUX+K7u4ifrZlQvj/81M4INjtXreqDiJtr99Rs6xa0ScZqITuZC4CWxJa9GynBE
D3+D2t1V/f810smsuYoFOF7Ib49IkTdbtWAtHlZp8bEhELBeGaPdNCcmfZ66rKud
G5sRA/9ovnc1krSQF2+sqB9/o7w5/q2qiyzwoSTnkjtBUVKn4zLUOf6aeBAoV6NM
```

## Mail server administrators should seriously consider upgrading their servers (Linux Reviews)

```
CC3Kj9aZHfA+ND0ehPaVGJgjaVNFhPi4x0e7BULdvgOoAqajLfvkURHAEsSxXIoE
myW/xC1sBbDkDUIBSx5oej73XCZgnj/inphRqGpsb+1nKFvF+rQoU3VTRSbQYWNr
YWdlIFNpZ25pbmcgS2V5IDxidWlsZEBzdXNlLmRlPohcBBMRAGAcBQI57vSBBQkD
wmcABAsKAwQDFQMCAXYCAQIXgAAKCRCoTt ronIAKYl8sAJ98BgD40zw0GHJHIf6d
NfnwI2PAsGcgjh1+PnYE17TFjtZsqhezX7vZvYCIrGQQEQIABGUCOnBeUgAKCRCE
QOMQAqrpnZOAKCL512FZvv4VZx94TpbA9lxyoAejACe001HtActAevk5MUBhNe
LZa/qM2JARUDBRA6cGBvd7LmAD0109kBATWnB/9An5vfiUUE1VQnt+T/EYk1ES3t
XXaJjp9pHMa4fzFa8jPvtv5UBHGee3XoUNdVwM2OgSEISZxbzdXGnqI1cT08TzBU
D9i579uifklLsnr35SJDZ6ram51/CWOnnaVhUzneOA9gTPSr+/ft3WeVnwJiQCQ3
0kNLWVXWATMnsnt486eAO1T6UNBPYQLpUprF5Yryk23pQUPAgJENDEqeU6iIO9Ot
1ZPtB0lniw+/xCi13D3660o1tZDYOp0hHHJN3D3EN8C1yPqZd5CvvznYvB6bWBIPW
cRgdn2DUVMmpU661jwqG1Rz1F84JG/xe4jGuzgpJt9IXSzyohEJB6XG5+D0BiF0E
ExECAB0FAjxqqTQFCQoAgrMFCwCkAwQDFQMCAXYCAQIXgAAKCRCoTt ronIAKyp1f
AJ9dR7saz2KPNwD3U+fy/0BDKXrYGACfbJ8fQcJqCBQxeHvt9yMPDVq0B0W5Ag0E
Oe70khAIAISR0E3ozF/la+oNaRwxHLrCet30NgnxRROYhPaJB/Tu1FQokn2/Qld/
HZnh3TwhBIwlFqrhWBJ7491iAjLR9uPbdWJrn+A7t8kSkPaF3Z/6kyc5a8fas44h
t5h+6HMBzoFCMAQ2aBHQRFRNp9Mz1ZvoXXc11k1180qcUM/ovXbDFPcXsUVeTPT
tGzcAi2jV19hl3iwJKkyv/RLmcusdsi8YunbvWGF5GaagYQo7Y1F6UaBQnYJTM
523AMgpPQtsKm9o/w9WdgXkgWhgkhZEeqUS3m5xNey1nLu9iMvq9M/iXnGz4sg6Q
2Y+GqZ+yAvNWjRRou3zSE7Bzg28MI4sAAwYH/2D71Xc5HPDgu87WnBFgmp8MpSr8
QnSs0wwPg3xEullGEocolSb2c0ctuSyeVnCttJMzkukL9TqyF4s/6XRstWirSWaw
JxRLKH6Zjo/FaKsshYkF8gBkAaddvpl3p00gmUYbqmpQ3xDEYlhCeieXS5MkockQ
1sj2xYdB1x00ExzfiCiscUKjUFy+mdzUsUtafuZ+gbHog1CN/ccZCkxcBa5IFCH
ORrnJq9pYwlrXsEn6ApsG7JJbM2besW1PkdEoxak74z1senh36m5jQvVjA3U4xq1
ewylxadmmJaJHzeiLfb7G1ZRjZTsB7fyYxqDzMVul6o9BSwO/1XsIANv1uuITAQY
EQIADAUC0e70kgUJA8JnAAKCRCoTt ronIAKYksIAJSFB3/77SkH3JLYOGrEe10L
0JdGwACEKtTttgeVFPF+iGJdiwQlxasOfuXyITAQYEQIADAUCPGqpWQUJCGcCxAk
CRCoTt ronIAKyofBAKCSZM2UFyta/fe9WgITK9I5hbxxTQCfX+0ar2CZmSknn3co
SPihnl+OBnyZAQ0DnuEtBAAAAQgAoCRcd7SVZEFcumffYewfLTcXQjhKzOahzXpo
omuF+HIyU4AGq+SU8sTZ/1SsjhdzrSAfv11ETACA+3SmLr5KV40Us1w0UC64cwt
A46xowVq1vMlH2Lib+V/qr3blhE67nMHjysECVx90b4gFuKNoR2eqnAaJvJnAT8J
/LoUC20EdCHUqn6v+M9t/WZgC+WNR8cq69uDY3YQhDP/nIan6fm2uf2kSV9A7ZxE
GrswW1/WX5Q/sQqMwaU6r4az98X3z90/cn+eJJ3vvtA+rm+nxEvyyev+jaLuOQBDf
ebh/XA4FZ35xmi+spdiVeJH4F/ubaGlmj7+wDOF3suYAPSXT2QAFEBQ1U3VTRSBT
ZWN1cml0eSBUZWFtIDxzZWN1cml0eUBzdXNlLmRlPohcBBMRAGAcBQI57vSBBQkD
RQEBVw4H/1vIdiOLX/7hdzYaG9crQVIk3QwaB5eBbjvLEMvuCZH1Y2COUG5QdmPQ
8S1WNZ6k4nu1BLcv2g/pymPUWP9fG4tuSn1UJDrWGM3nhyhAC9iudP2ulYQY37Gb
B6NPVaZiYmEb4QYfcqv5c/r2ghSXUTYk7etd6SW6WCOpEqizhx1cqDKNZnsI/1X
11pFc02N7rc6byDBJ1T+cK+F1Ehan9XBt/shryJmv04nli5CXQMEbiqYYMOu8iaA
8AWRgXPCWqhyGhcVD3LRhUJXjUOdH4ZiHCXaoF3zVPxpeGKEQY8iBrDeDyB3wHmj
qY9WCX6cmogGQRgY6yJqDalLqrDODmJARUDBRA24S0Ed7LmAD0109kBAW04B/4p
WH3flvQn3i6/+SmDjGzUu2GWGq6Fsdwo2hVM2ym6CILEow/K9JfhdwGvY8LRxWRL
hn09j2IJ9P7H1Yz3qDf10AX6V7YILHtchKT1dcngCkTLmDgC4rs1iAA13f089sRG
BafGPGKv2DQjhfR1Lfrtbf0P7c09Tkej1MP8HtQMW9hPkBYeXcwbCjdrVGFozqx+
AvvJDDt6a+oyRMTflvmZ83UV5pgoyimgjhWnM1V4bFBJpPrtWmkdXJSUXbR6Q7Pi
RZWCzGRzwbaxqpl3rK/YTCphOLwEMB27B4/fcqtBzgoMOiaZA0M5ffF0o54KgRiH0
zinsSx2OrWgvSILEXXYkiEYEEBECAAYFAjseYcMACgkQnkDjEAAKq6ROVACgjhDM
/3KM+iFjs5QXsnd4oFPOnbkAnjYGalJ3em+bmV2aiCdYXDOuGn4ZiQCVAwUQN7c7
whaQN/7O/JIVAQEB+QP/cyblSAmPXxSFiaHWB+MiUNw8B6ozBLK0QcMQ2YcL6+V1
D+nSZP20+Ja2nfiKjnibCv5ss83yXoHkYk2Rsa8foz6Y7tHwuPiccvqnIC/c9Cvz
dbIsdxpfsi0qWpFvX/jLmpXqqnPjdIZErgxpwuJas1n9016PuXA8K3MJwVjCqSKI
RgQQEQIABGUCOHPcPAAKCRDHUqoysN/3gCt7AJ9adNQMbma1iSYcbhtgvx9ByLPI
DgCfZ5Wj+f7cnYpFZI6GkAyyczG09sE=
=LRKC
```

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

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

Version: GnuPG v1.2.4 (GNU/Linux)

```
iQEVAwUBQiQ1R3ey5gA9JdPZAQFDtgf9HkBJxAGeeHRg/18nVzSBE8iUYOf1Qeua
aTAMX1lG24yEpnnZ0iemhTwLpEsqQtViDxQrh1x1jXGJCGR0PcIEejadbVq6vzF
KHDxxIDRnUsy7EiTjZrD32G0n956BCwM13AjrFPz1IcUXnchA98oLTKbd7J/z8F/
```

## Mail server administrators should seriously consider upgrading their servers (Linux Reviews)

```
ZDquwyrnl0yb8fcwb0VlXhcxVVEuJmvHT3Jh4qGfK9xJAzWETkauXnEmlE3cmaKN
OC3h15oofxoW7kAE1t2/3iEa2T+vzFXc4SAorwo2zOVxIFyWLEM361ZgBtkyK+Qe
IW38o1LRRU6Lq5FJ5aHty6HUITXF5ZoK7KbqXgYs7KBdpkcPG66POA==
=K0X8
-----END PGP SIGNATURE-----
```

```
--
To unsubscribe, e-mail: suse-security-announce-unsubscribe@suse.com
For additional commands, e-mail: suse-security-announce-help@suse.com
```

```
...
```

## 2. Cyrus-imapd, Suse announcement

```
...
-----BEGIN PGP SIGNED MESSAGE-----
```

---

### SUSE Security Announcement

```
Package:                cyrus-imapd
Announcement-ID:        SUSE-SA:2005:009
Date:                   Thu, 24 Feb 2005 14:00:00 +0000
Affected products:     8.2, 9.0, 9.1, 9.2
                        SUSE Linux Enterprise Server 8, 9
Vulnerability Type:    remote code execution
Severity (1-10):        7
SUSE default package:  yes
Cross References:       None.
```

#### Content of this advisory:

- 1) security vulnerability resolved:  
several 1 byte buffer overflows fixed
- 2) solution/workaround
- 3) special instructions and notes
- 4) package location and checksums
- 5) pending vulnerabilities, solutions, workarounds:  
See SUSE Security Summary Report.
- 6) standard appendix (further information)

---

#### 1) problem description, brief discussion

This update fixes one-byte buffer overruns in the cyrus-imapd IMAP server package.

Several overruns were fixed in the IMAP annotate extension as well as in cached header handling which can be run by an authenticated user.

Additionally bounds checking in fetchnews was improved to avoid exploitation by a peer news admin.

Please note that one-byte buffer overflows can not be exploited to

## Mail server administrators should seriously consider upgrading their servers (Linux Reviews)

execute arbitrary commands by manipulating the saved registers on the stack if the compiler used (`gcc >= 3`) aligns the stack space.

Nevertheless the code behavior may be manipulated by overwriting local variables. The result is not known but ranges between a denial-of-service condition and privilege escalation.

This update backports bugfixes from the upstream release of `cyrus-imapd 2.2.11` announced on:

<http://asg.web.cmu.edu/archive/message.php?mailbox=archive.info-cyrus&msg=33723>

### 2) solution/workaround

Install the updated packages.

Make sure you restart `cyrus-imapd` by running  
`/sbin/rccyrus try-restart`

### 3) special instructions and notes

None.

### 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/cyrus-imapd-2.2.8-6.5.i586.rpm`  
`3bfbec25eb82d07a8195fb621876cf4b`

##### SUSE Linux 9.1:

`ftp://ftp.suse.com/pub/suse/i386/update/9.1/rpm/i586/cyrus-imapd-2.2.3-83.22.i586.rpm`  
`e90855625f9d66bed10f0d601517ca7f`

##### SUSE Linux 9.0:

`ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/i586/cyrus-imapd-2.1.15-91.i586.rpm`  
`b3f0a8e7ab5780b2544a2c5ce9671b18`

##### SUSE Linux 8.2:

`ftp://ftp.suse.com/pub/suse/i386/update/8.2/rpm/i586/cyrus-imapd-2.1.12-77.i586.rpm`  
`989a125263e4388b2e3825262e495923`

#### x86-64 Platform:

##### SUSE Linux 9.2:

`ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/x86_64/cyrus-imapd-2.2.8-6.5.x86_64.rpm`  
`267540ff1676d534dc0bab3b075a0b32`

##### source rpm(s):

`ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/src/cyrus-imapd-2.2.8-6.5.src.rpm`  
`8f78ab5817abd9a354473a6f10f6c5d5`

##### SUSE Linux 9.1:

`ftp://ftp.suse.com/pub/suse/x86_64/update/9.1/rpm/x86_64/cyrus-imapd-2.2.3-83.22.x86_64.rpm`

## Mail server administrators should seriously consider upgrading their servers (Linux Reviews)

```
0b51738a00dbb8cc71d1277d1b370576
source rpm(s):
ftp://ftp.suse.com/pub/suse/x86_64/update/9.1/rpm/src/cyrus-imapd-2.2.3-83.22.src.rpm
    b1316bfae2476c5e880e581893cad224
```

```
SUSE Linux 9.0:
ftp://ftp.suse.com/pub/suse/x86_64/update/9.0/rpm/x86_64/cyrus-imapd-2.1.15-91.x86_64.rpm
    4c5bc7aa5de6ca5a9ef2758b17b20ba3
source rpm(s):
ftp://ftp.suse.com/pub/suse/x86_64/update/9.0/rpm/src/cyrus-imapd-2.1.15-91.src.rpm
    c6ce2fd455ddc73b00e4092b5332335f
```

---

### 5) Pending vulnerabilities in SUSE Distributions and Workarounds:

See SUSE Security Summary Report.

---

### 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

## Mail server administrators should seriously consider upgrading their servers (Linux Reviews)

~/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>.  
@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+2vv4MGVKiLEMO19GdST6MCKYS3yEKeueNWc+z/0Kvff
4JctBsgs47tjmiI9s10eHjm3gTR8rItXMN6sJEUHWzDP+Y0PFPboMvKx0FX1/A0d
M+HFrruCGBlWt6FA+okRySQiliuI5phwqkXefl9AhkWR8xocQSVCFxcwvvcg1VcO
QliHu8jwRQHx1RE0tkwQOI0D+wfQwKdvhDplxHJ5nf7U8c/yE/vdvpN61F0tmFrK
XBUX+K7u4ifrZlQvj/81M4INjtXreqDiJtr99Rs6xa0ScZqITuZC4CWxJa9GynBE
D3+D2t1V/f810smsuYoFOF7Ib49IkTdbtWAtHlZp8bEhELBeGaPdNCcmfZ66rKud
G5sRA/9ovnc1krSQF2+sqB9/o7w5/q2qiyzWOSTnkjtBUVKn4zLUOf6aeBAoV6NM
```

## Mail server administrators should seriously consider upgrading their servers (Linux Reviews)

```
CC3Kj9aZHfA+ND0ehPaVGJgjaVNFhPi4x0e7BULdvgOoAqajLfvkURHAEsSxXIoE
myW/xC1sBbDkDUIBSx5oej73XCZgnj/inphRqGpsb+1nKFvF+rQoU3VTRSbQYWNr
YWdlIFNpZ25pbmcgS2V5IDxidWlsZEBzdXNlLmRlPohcBBMRAGAcBQI57vSBBQkD
wmcABAsKAwQDFQMCAXYCAQIXgAAKCRCoTt ronIAKYl8sAJ98BgD40zw0GHJHIf6d
NfnwI2PAsGcgjh1+PnYEl7TFjtZsqhezX7vZvYCIrGQQEQIABGUConBeUgAKCRCE
QOMQAqrpnZOAKCL512FZvv4VZx94TpbA9lxyoAejAcE001HtActAevk5MUBhNe
LZa/qM2JARUDBRA6cGBvd7LmAD0109kBATWnB/9An5vfiUUE1VQnt+T/EYk1ES3t
XXaJjp9pHMa4fzFa8jPvtv5UBHGee3XoUNdVwM2OgSEISZxbzdXGnqI1cT08TzBU
D9i579uifklLsnr35SJDZ6ram51/CWOnnaVhUzneOA9gTPSr+/ft3WeVnwJiQCQ3
0kNLWVXWATMnsnt486eAO1T6UNBPYQLpUprF5Yryk23pQUPAgJENDEqeU6iIO9Ot
1ZPtB0lniw+/xCi13D3660o1tZDYOp0hHHJN3D3EN8C1yPqZd5CvvznYvB6bWBIPW
cRgdn2DUVMmpU661jwqG1Rz1F84JG/xe4jGuzgpJt9IXSzyohEJB6XG5+D0BiF0E
ExECAB0FAjxqqTQFCQoAgrMFCwCkAwQDFQMCAXYCAQIXgAAKCRCoTt ronIAKyp1f
AJ9dR7saz2KPNwD3U+fy/0BDKXrYGACfbJ8fQcJqCBQxeHvt9yMPDVq0B0W5Ag0E
Oe70khAIAISR0E3ozF/la+oNaRwxHLrCet30NgnxRROYhPaJB/Tu1FQokn2/Qld/
HZnh3TwhBIwlFqrhWBj7491iAjLR9uPbdWJrn+A7t8kSkPaF3Z/6kyc5a8fas44h
t5h+6HMBzoFCMAQ2aBHQRFRNp9Mz1ZvoXXc11k1180qcUM/ovXbdfPcXsUVeTPT
tGzcAi2jV19hl3iwJKkyv/RLmcusdsi8YunbvWGFaf5GaagYQo7Y1f6UaBQnYJTM
523AMgpPQtsKm9o/w9WdgXkgWhgkhZEqUS3m5xNey1nLu9iMvq9M/iXnGz4sg6Q
2Y+GqZ+yAvNWjRRou3zSE7Bzg28MI4sAAwYH/2D71Xc5HPDgu87WnBFgmp8MpSr8
QnSs0wwPg3xEullGEocolSb2c0ctuSyeVnCttJMzkukL9TqyF4s/6XRstWirSWaw
JxRLKH6Zjo/FaKsshYkF8gBkAaddvpl3p00gmUYbqmpQ3xDEYlhCeieXS5MkockQ
1sj2xYdB1x00ExzfiCiscUKjUFy+mdzUsUtafuZ+gbHog1CN/ccZCkxcBa5IFCH
ORrnJq9pYwlrXsEn6ApsG7JJBm2besW1PkdEoxak74z1senh36m5jQvVjA3U4xq1
wylxadmmJaJHzeiLfb7G1ZRjZTsB7fyYxqDzMVul6o9BSwO/1XsIANv1uuITAQY
EQIADAUCOe70kgUJA8JnAAKCRCoTt ronIAKYksiaJsfB3/77SkH3JLYOGrEe10L
0JdGwACEKtTttgeVFPFB+iGJdiwQlxasOfuXyITAQYEQIADAUCPGqPwQUJcGcCxAk
CRCoTt ronIAKyofBAKCSZM2UFyta/fe9WgITK9I5hbxxTQCfX+0ar2CzmSknn3co
SPihnl+OBnyZAQ0DnuEtBAAAAQgAoCRcd7SVZEFcumffYewfLTcXQjhKzOahzXpo
omuF+HIYU4AGq+SU8sTZ/1SsjhdzrSAfv11ETACA+3SmLr5KV40Us1w0UC64cwt
A46xowVq1vMlH2Lib+V/qR3blhE67nMHjysECVx90b4gFuKNOR2eqnAaJvJnAT8J
/LoUC20EdCHUqn6v+M9t/WZgC+WNR8cq69uBy3YQhDP/nIan6fm2uf2kSV9A7ZxE
GrswW1/WX5Q/sQqMwaU6r4az98X3z90/cn+eJJ3vvtA+rm+nxEvyeV+jaLuOQBdf
ebh/XA4FZ35xmi+spdiVeJH4F/ubaGlmj7+wDOF3suYAPSXT2QAfEbQ1U3VTRSbT
ZWN1cml0eSBUZWFtIDxzZWN1cml0eUBzdXNlLmRlPohcBBMRAGAcBQI57vSBBQkD
RQEBVw4H/1vIdiOLX/7hdzYaG9crQVIk3QwaB5eBbjvLEMvuCZH1Y2COUG5QdmPQ
8S1WNZ6k4nu1BLcv2g/pymPUWP9fg4tuSn1UJDrWGM3nhyhAC9iudP2ulYQY37Gb
B6NPVaZiYmEb4QYfcqv5c/r2ghSXUTYk7etd6SW6WCOpEqizhx1cqDKNZnsI/1X
11pFc02N7rc6byDBJ1T+cK+F1Ehan9XBt/shryJmv04nli5CXQMEbiqYYMOu8iaA
8AWRgXPCWqhyGhcVD3LRhUJXjUOdH4ZiHCXaoF3zVPxpeGKEQY8iBrDeDyB3wHmj
qY9WCX6cmogGQRgY6yJqDalLqrDODmJARUDBRA24S0Ed7LmAD0109kBAW04B/4p
WH3flvQn3i6/+SmDjGzUu2GWGq6Fsdwo2hVM2ym6CILEow/K9JfhdwGvY8LRxWRL
hn09j2IJ9P7H1Yz3qDf10AX6V7YILHtchKT1dcngCkTLmDgC4rs1iAA13f089sRG
BafGPGKv2DQjhfR1Lfrtbf0P7c09Tkej1MP8HtQMW9hPkBYeXcwbCjdrVGFozqx+
AvvJDDt6a+oyRMTflvmZ83UV5pgoyimgjhWnM1V4bFBYjprtWmkdXJSUXbR6Q7Pi
RZWCzGRzwbaxqpl3rK/YTCphOLwEMB27B4/fcqtBzgoMOiaZA0M5ffF0o54KgRIh0
zinsSx2OrWgVSiLEXXYKiEYEEBECAAYFAjseYcMACgkQnkDjEAAKq6ROVACgjhDM
/3KM+iFjs5QXsnd4oFPOnbkAnjYGalJ3em+bmV2aiCdYXdOuGn4ZiQCVawUQN7c7
whaQN/7O/JIVAQEB+QP/cYblSAmPXxSFiaHWB+MiUNw8B6ozBLK0QcMQ2YcL6+V1
D+nSZP20+Ja2nfiKjnibCv5ss83yXoHkYk2Rsa8foz6Y7tHwuPiccvqnIC/c9Cvz
dbIsdxpfsi0qWpFvX/jLmpXqqnPjdIZErgxpwuJas1n9016PuXA8K3MJwVjCqSKI
RgQQEQIABGUConhpCpAAKCRDHUqoysN/3gCt7AJ9adNQMbma1iSYcbhtgvx9ByLPI
DgCfZ5Wj+f7cnYpFZI6GkAyyczG09sE=
=LRKC
```

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

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

Version: GnuPG v1.2.4 (GNU/Linux)

```
iQEVAwUBQh32yHey5gA9JdPZAQG1Mgf/VJNvZRkqx6bFLXihg/oXuCsPaE9vgJBT
DaSbpxVx0v+goK+etByCiN70NZWseqOpBYZOBnJTGbIu4VYGNiZZ6CFVHlzZIGkv
VTD+1QBQoK5M3aQ88RSbYpmtb6fPbOH+nJ2sIEKaX0JJ8iZp4v87KRTTanmN7tRf
```

## Mail server administrators should seriously consider upgrading their servers (Linux Reviews)

qSKCwrNkMSuMQ6pD4dfTasHk3AdnBJfvMva0alfyuqvXoLu8w1UYf+eJQvzk+24w  
iqi+Afl/+pVM7Orpvj3yg8L64gJRh+52iHpnL8GU//S7cTGYIkc/HT1KAY9Ecw25  
EBuwdBRqd3Inj8D5l6csb0ptQZ7H0ktrbhpVKNJOUYfH45FL4se6tg==  
=LJ7l

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

--

To unsubscribe, e-mail: [suse-security-announce-unsubscribe@suse.com](mailto:suse-security-announce-unsubscribe@suse.com)

For additional commands, e-mail: [suse-security-announce-help@suse.com](mailto:suse-security-announce-help@suse.com)

^^^

---

> [Linux Reviews](#) > [News and headlines](#) > [2005 News archive](#) > [March](#) >

Mail server administrators should seriously consider upgrading their servers