

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,
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)

1) problem description, brief discussion

The University of Washington imap daemon can be used to access 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 an arbitrary user.

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

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. They 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-20050201-1.1.i586.rpm
2b4cf0f70fb0164a90f6e73b66f28c5a

SUSE Linux 9.1:

ftp://ftp.suse.com/pub/suse/i386/update/9.1/rpm/i586/imap-20050201-1.1.i586.rpm
32eb45928cf31bb0cbae78139303561b

SUSE Linux 9.0:

ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/i586/imap-20050201-1.1.i586.rpm
b8af4a9008cb1d311f650700b6d642c5

SUSE Linux 8.2:

ftp://ftp.suse.com/pub/suse/i386/update/8.2/rpm/i586/imap-20050201-1.1.i586.rpm
6f73b1197b2a095fc30b8afde860f5fe

x86-64 Platform:

SUSE Linux 9.2:

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

```
ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/x86_64/imap-  
a6a79a3e1459dd1d5799e40257684d4e
```

```
source rpm(s):
```

```
ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/src/imap-200  
18201a6f78b73d2250f6ea0e614049b2
```

```
SUSE Linux 9.1:
```

```
ftp://ftp.suse.com/pub/suse/x86_64/update/9.1/rpm/x86_64/ima  
007c9777aacc36dec72067cf6ac39e7d
```

```
source rpm(s):
```

```
ftp://ftp.suse.com/pub/suse/x86_64/update/9.1/rpm/src/imap-2  
9bf8dda300636e712f164d784bc131a5
```

```
SUSE Linux 9.0:
```

```
ftp://ftp.suse.com/pub/suse/x86_64/update/9.0/rpm/x86_64/ima  
25ffa1aa178c962753bc26483d0e9354
```

```
source rpm(s):
```

```
ftp://ftp.suse.com/pub/suse/x86_64/update/9.0/rpm/src/imap-2  
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 around the world. While this service is being considered valuable and useful to the free and open source software community, many users will not 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 file or rpm package:

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

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

- 1) execute the command

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

after you downloaded the file from a SUSE ftp server or i
Then, compare the resulting md5sum with the one that is l
announcement. Since the announcement containing the check
cryptographically signed (usually using the key security@
the checksums show proof of the authenticity of the packa
We disrecommend to subscribe to security lists which caus
email message containing the announcement to be modified
the signature does not match after transport through the
list software.

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

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

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

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

Prerequisites:

- a) gpg is installed
- b) The package is signed using a certain key. The public
key must be installed by the gpg program in the direct
~/.gnupg/ under the user's home directory who perform
signature verification (usually root). You can import
that is used by SUSE in rpm packages for SUSE Linux b
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 i  
key "build@suse.de" upon installation or upgrade, pro  
the package gpg is installed. The file containing the  
is placed at the top-level directory of the first CD  
and at ftp://ftp.suse.com/pub/suse/pubring.gpg-build.
```

- SUSE runs two security mailing lists to which any interested

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

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

- -----BEGIN PGP PUBLIC KEY BLOCK-----
 Version: GnuPG v1.0.6 (GNU/Linux)
 Comment: For info see http://www.gnupg.org

mQGIBDnu9IERBACT8Y35+2vv4MGVKiLEMO19GdST6MckYS3yEKeueNWc+z/0Kvff

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

4JctBsgs47t jmiI9sl0eHjm3gTR8rItXMN6sJEUHWzDP+Y0PFPboMvKx0FX1/A0c
M+HFrruCGBlWt6FA+okRySQilIuI5phwqkXefl9AhkwR8xocQSVCFxcwvwCglVcC
QliHu8jwRQHxlRE0tkwQQI0D+wfQwKdvhDplxHJ5nf7U8c/yE/vdvpN6lF0tmFrK
XBUX+K7u4ifrzlQvj/8lM4INjtXreqDiJtr99Rs6xa0ScZqITuZC4CWxJa9GynBE
D3+D2t1V/f8l0smsuYoFOF7Ib49IkTdbtwATHlZp8bEhELBeGaPdNCcmfZ66rKU
G5sRA/9ovnc1krSQF2+sqB9/o7w5/q2qiyzwoSTnkjtBUVKn4zLUOf6aeBAoV6NM
CC3Kj9aZHfA+ND0ehPaVGJgjaVNFhPi4x0e7BULdvgOoAqajLfvkURHAeSsxXI0E
myW/xC1sBbDkDUIBSx5oej73XCZgnj/inphRqGpsb+1nKFvF+rQoU3VTRSBQYWNr
YWdlIFNpZ25pbmcgS2V5IDxidWlsZEBzdXNlLmRlPohcBBMRAgAcBQI57vSBBQkD
wmcABAsKAwQDFQMCAxYCAQIXgAAKCRCoTtronIAKy18sAJ98BgD40zw0GHJHI6c
NfnwI2PAsgCgjH1+PnYE17TFjtZsqhezX7vZvYCIrGQQEQIABgUCOnBeUgAKCRCe
QOMQAAqrpnzoAKCL512FZvv4VZx94TpbA91xyoAejACE001HIbActAevk5MUBhNe
Lza/qM2JARUDBRA6cGBvd7LmAD0109kBATWnB/9An5vfiUUE1VQnt+T/EYklES3t
XXaJJP9pHMa4fzFa8jPVtv5UBHGee3XoUNdVwM2OgSEISZxbzdXGnqIlct08TzBU
D9i579uifklLsnr35SJDZ6ram51/CWOnnaVhUzneOA9gTPSr+/ft3WeVnwJiQCQ3
0kNLWVXWATMnsnt486eA01T6UNBPYQLpUprf5Yryk23pQUPAgJENDEqeU6iIO9Ot
1ZPtB0lniw+/xCi13D360o1tZDYOp0hHHJN3D3EN8C1yPqZd5CvvznYvB6bWBIPW
cRgdn2DUVMmpU661jwqG1Rz1F84JG/xe4jGuzgpJt9IXSzyohEJB6XG5+D0BiFOE
ExECAB0FAjxqqTQFCQoAgrMFCwcKAwQDFQMCAxYCAQIXgAAKCRCoTtronIAKyp1f
AJ9dR7saz2KPNwD3U+fy/0BDKXrYGACfbJ8fQcJqCBQxeHvt9yMPDVq0B0W5Ag0E
Oe70khAIAISR0E3ozF/la+oNaRwxHLrCet30NgnxRR0YhPaJB/Tu1FQokn2/Qld/
HZnh3TwhBIw1FqrhWBJ7491iajLR9uPbdWJrn+A7t8kSkPaF3Z/6kyc5a8fas44h
t5h+6HMBzoFCMAq2aBHQRFRNp9Mz1ZvoXXcI11k1180qcUM/ovXbDfPcXsUVEPT
tGzcAi2jVl9h13iwJKkyv/RLmcusdsi8YunbvWGFAF5GaagYQo7Y1f6UaBQnYJTM
523AMgpPQtsKm9o/w9WdgXkgWhgkhZEeqUS3m5xNey1nLu9iMvq9M/iXnGz4sg6Q
2Y+GqZ+yAvNWjRRou3zSE7Bzg28MI4sAAwYH/2D71Xc5HPDgu87WnBFgmp8MpSr8
QnSs0wwPg3xEu1lGEocolSb2c0ctuSyeVnCttJMzkukL9TqyF4s/6XRstWirSWaw
JxRLKH6Zjo/FaKsshYKf8gBkAaddvpl3p00gmUYbqmpQ3xDEYlhCeieXS5MkockQ
1sj2xYdB1x00ExzfiCiscUKjUFy+mdzUsUutaFuZ+gbHog1CN/ccZCkxcBa5IFCH
ORrnjq9pYwlrxsEn6ApsG7JJBm2besW1PkdEoxak74z1senh36m5jQvVjA3U4xq1
wwylxadmmJaJHzeiLfb7G1ZRjZTsB7fyYxqDzMVul6o9BSwO/1XsIAnV1uuITAQY
EQIADAUCOe70kgUJA8JnAAAKCRCoTtronIAKyksiAJsFB3/77SkH3J1YOGrEe10J
0JdGwACeKTttgeVPFB+igJdiwQlxasOfuXyITAQYEQIADAUCPGqpWQUJCgCCxwAK
CRCoTtronIAKyofBAKCSZM2UFyta/fe9WgITK9I5hbxxTQCfX+0ar2CZmSknn3cc
SPihnl+OBnyZAQ0DNuEtBAAAAQgAoCRcd7SVZEFcumffYEwflTcXQjhKzOahzxp
omuF+HIyU4AGq+SU8sTZ/1SsjhdzZRSAfv11ETACA+3SmLr5KV40Us1w0UC64cwt
A46xowVq1vMlH2Lib+V/qr3b1hE67nMHjysECVx9Ob4gFuKNoR2eqnAaJvjnAT8J
/LoUC20EdCHUqn6v+M9t/WZgC+WNR8cq69uDy3YQhDP/nIan6fm2uf2kSV9A7Zx
GrwsWl/WX5Q/sQqMwaU6r4az98X3z90/cN+eJJ3vwtA+rm+nxEvyeV+jaLuOQBDf
ebh/XA4FZ35xmi+spdiVeJH4F/ubaGlmj7+wDOF3suYAPSXT2QAFebQ1U3VTRSBT
ZWN1cml0eSBUZWFtIDxzZWN1cml0eUBzdXNlLmRlPokBFQMFEDbhLUfkWLKHsco8
RQEBVw4H/1vIdiOLX/7hdzYaG9crQVIk3QwaB5eBbjvLEMvuCZHiY2COUG5QdmPQ

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

```
8SlWNZ6k4nu1BLcv2g/pymPUWP9fG4tuSn1UJDrWGm3nhyhAC9iudP2u1YQY37Gh
B6NPVaziYMnEb4QYFcqv5c/r2ghSXUTYk7etd6SW6WCOPEqizhx1cqDKNZnsI/1X
11pFcO2N7rc6byDBJ1T+cK+F1Ehan9XBt/shryJmv04nli5CXQMEbiqYYMOu8iaA
8AWRgXPCWqhyGhcVD3LRhUJXjUOdH4ZiHCXaoF3zVPxpeGKEQY8iBrDeDyB3wHm
qY9WCX6cmogGQRgYG6yJqDalLqrDOdmJARUDBRA24S0Ed7LmAD0109kBAW04B/4p
WH3f1vQn3i6/+SmDjGzUu2GWGq6Fsdwo2hVM2ym6CILEow/K9JfhdwGvY8LRxWR
hn09j2IJ9P7H1Yz3qDf10AX6V7YILHtchKT1dcngCkTLMdGc4rs1iAA13f089sR
BafGPGKv2DQjHfR1Lfrtbf0P7c09Tkej1MP8HtQMW9hPkBYeXcwbCjdrVGFOzqx+
AvvJDDt6a+oyRMTFlvmZ83UV5pgoyimgjhWnM1V4bFByjPrtWMkdXJSUXbR6Q7Pi
RZWCzGRzwbaxqpl3rK/YTCphOLwEMB27B4/fcqtBzgoMOiaZA0M5fF0o54KgRIhC
zinsSx2OrWgvSiLEXXYKiEYEEBECAAYFAjseYcMACgkQnkDjEAAKq6ROVACgjhDM
/3KM+iFjs5QXsnd4oFPOnbkAnjYGalJ3em+bmV2aiCdYXdOuGn4ZiQCVAwUQN7c7
whaQN/70/JIVAQEB+QP/cYblsAmPxxSFiaHWB+MiUNw8B6ozBLK0QcMQ2YcL6+VL
D+nSZP20+Ja2nfiKjnibCv5ss83yXoHkYk2Rsa8foz6Y7tHwuPiccvqnIC/c9Cvz
dbIsdxpfsi0qWPfvX/jLMpXqqnPjdIZErgxpwuja1n9016PuXA8K3MJwVjCqSKL
RgQQEQIABgUCOhpCpAAKCRDHUqoysN/3gCt7AJ9adNQMbma1iSYcbhtgvx9ByLP
DgCfZ5Wj+f7cnYpFZI6GkAyyyczG09sE=
=LRKC
```

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

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

Version: GnuPG v1.2.4 (GNU/Linux)

```
iQEVAwUBQiQ1R3ey5gA9JdPZAQFDtgf9HkBjxAGeeHRg/18nVzSBE8iUYOf1Qeua
aTAMX1lG24yEpnnZ0iemhTwLpEsqQttViDxQrh1x1jXGJCgR0PcIEejadbVq6vzE
KHDxxIDRnUsy7EiTjZrD32G0n956BCwMl3AjrfPz1IcUXnchA98oLTKbd7J/z8F/
ZDquwyrnl0yb8fcwb0VlXhcxVVEuJmvHT3Jh4qGfK9xJAzWETkauXnEm1E3cmaKN
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,
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 server package.

Several overruns were fixed in the IMAP annotate extension as in cached header handling which can be run by an authenticat

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

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

Nevertheless the code behavior may be manipulated by overwriting local variables. The result is not known but ranges between 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.i>

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 get the update.

Our maintenance customers are being notified individually. They 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-i>

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

3bfbec25eb82d07a8195fb621876cf4b

SUSE Linux 9.1:

ftp://ftp.suse.com/pub/suse/i386/update/9.1/rpm/i586/cyrus-imapd-2.2.12-1.1.i586.rpm
e90855625f9d66bed10f0d601517ca7f

SUSE Linux 9.0:

ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/i586/cyrus-imapd-2.2.12-1.1.i586.rpm
b3f0a8e7ab5780b2544a2c5ce9671b18

SUSE Linux 8.2:

ftp://ftp.suse.com/pub/suse/i386/update/8.2/rpm/i586/cyrus-imapd-2.2.12-1.1.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-2.2.12-1.1.x86_64.rpm
267540ff1676d534dc0bab3b075a0b32

source rpm(s):

ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/src/cyrus-imapd-2.2.12-1.1.src.rpm
8f78ab5817abd9a354473a6f10f6c5d5

SUSE Linux 9.1:

ftp://ftp.suse.com/pub/suse/x86_64/update/9.1/rpm/x86_64/cyrus-imapd-2.2.12-1.1.x86_64.rpm
0b51738a00dbb8cc71d1277d1b370576

source rpm(s):

ftp://ftp.suse.com/pub/suse/x86_64/update/9.1/rpm/src/cyrus-imapd-2.2.12-1.1.src.rpm
b1316bfae2476c5e880e581893cad224

SUSE Linux 9.0:

ftp://ftp.suse.com/pub/suse/x86_64/update/9.0/rpm/x86_64/cyrus-imapd-2.2.12-1.1.x86_64.rpm
4c5bc7aa5de6ca5a9ef2758b17b20ba3

source rpm(s):

ftp://ftp.suse.com/pub/suse/x86_64/update/9.0/rpm/src/cyrus-imapd-2.2.12-1.1.src.rpm
c6ce2fd455ddc73b00e4092b5332335f

5) Pending vulnerabilities in SUSE Distributions and Workarounds

See SUSE Security Summary Report.

6) standard appendix: authenticity verification, additional info

- 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 useful to the free and open source software community, many users were not sure about the origin of the package and its content before downloading the package. There are two verification methods that can be used independently from each other to prove the authenticity of a file or rpm package:

- 1) md5sums as provided in the (cryptographically signed) announcements
- 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 mirror. 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@security.suse.com) the checksums show proof of the authenticity of the package. We disrecommend to subscribe to security lists which cause an email message containing the announcement to be modified. If 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 updated and a new version of a package is published on the ftp server, the 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 uninstalled package file.

Prerequisites:

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

- a) gpg is installed
- b) The package is signed using a certain key. The public key must be installed by the gpg program in the directory `~/.gnupg/` under the user's home directory who performs signature verification (usually root). You can import that key which is used by SUSE in rpm packages for SUSE Linux by running the command (do "su -" to be root):

```
gpg --batch; gpg < announcement.txt | gpg --import
```

SUSE Linux distributions version 7.1 and thereafter include this key "build@suse.de" upon installation or upgrade, provided the package gpg is installed. The file containing the key is placed at the top-level directory of the first CD-ROM and at `ftp://ftp.suse.com/pub/suse/pubring.gpg-build`.

- SUSE runs two security mailing lists to which any interested party can 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.
=====

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

The information in this advisory may be distributed or reproduced provided that the advisory is not modified in any way. In part 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
pub  1024D/9C800ACA 2000-10-19 SuSE Package Signing Key <build@s
```

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

Version: GnuPG v1.0.6 (GNU/Linux)

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

```
mQGIBDnu9IERBACT8Y35+2vv4MGVKiLEMO19GdST6MCKYS3yEKeueNWc+z/0Kvff
4JctBsgs47tjmiI9sl0eHjm3gTR8rItXMN6sJEUHWzDP+Y0PFPboMvKx0FX1/A0c
M+HFrruCGBlWt6FA+okRySQiliuI5phwqkXefl9AhkwR8xocQSVCFxcwvwCglVcQ
QliHu8jwRQHxlRE0tkwQQI0D+wfQwKdvhDplxHJ5nf7U8c/yE/vdvpN6lF0tmFrk
XBUX+K7u4ifrzlQvj/81M4INjtXreqDiJtr99Rs6xa0ScZqITuZC4CWxJa9GynBE
D3+D2t1V/f8l0smsuYoFOF7Ib49IkTdbtwAThlZp8bEhELBeGaPdNCcmfZ66rKUc
G5sRA/9ovnc1krSQF2+sqB9/o7w5/q2qiyzwOSTnkjtBUVKn4zLUOf6aeBAoV6NM
CC3Kj9aZHfA+ND0ehPaVGJgjaVNFhPi4x0e7BULdvgOoAqajLfvkURHAeSsxXI0E
myW/xClSbDkdUIBSx5oej73XCZgnj/inphRqGpsb+1nKFvF+rQoU3VTRSBQYWNr
YWdlIFNpZ25pbmcgS2V5IDxidWlsZEBzdXNlLmRlPohcBBMRAgAcBQI57vSBBQkD
wmcABAsKAwQDFQMCAxYCAQIXgAAKCRCoTtronIAKyl8sAJ98BgD40zw0GHJHI6c
NfnwI2PASgCgjH1+PnYEl7TFjtZsqhezX7vZvYCIrGQQEQIABgUCOnBeUgAKCRCe
QOMQAAqrpnzoAKCL512FZvv4VZx94TpbA9lxyoAejACE001HIbActAevk5MUBhNe
Lza/qM2JARUDBRA6cGBvd7LmAD0109kBATWnB/9An5vfiUUE1VQnt+T/EYk1ES3t
XXaJJP9pHMa4fzFa8jPvtv5UBHGee3XoUNdVwM2OgSEISZxbzdXGnqIlcT08TzBU
D9i579uifklLsnr35SJDZ6ram51/CWOnnaVhUzneOA9gTPSr+/ft3WeVnwJiQCQ3
0kNLWVXWATMnsnt486eA01T6UNBPYQLpUprF5Yryk23pQUPAgJENDEqeU6iIO90t
1ZPtB0lniw+/xCi13D360o1tZDYOp0hHHJN3D3EN8C1yPqZd5CvvznYvB6bWBIPw
cRgdn2DUVMmpU661jwqGlRz1F84JG/xe4jGuzgpJt9IXSzyohEJB6XG5+D0BiF0E
ExECAB0FAjxqqTQFCQoAgrMFCwckAwQDFQMCAxYCAQIXgAAKCRCoTtronIAKyp1f
AJ9dR7saz2KPNwD3U+fy/0BDKXrYGACfbJ8fQcJqCBQxeHvt9yMPDVq0B0W5Ag0E
Oe70khAIAISR0E3ozF/la+oNaRwxHLrCet30NgnxRR0YhPaJB/Tu1FQokn2/Qld/
HZnh3TwhBIw1FqrhWBJ7491iAjLR9uPbdWJrn+A7t8kSkPaF3Z/6kyc5a8fas44h
t5h+6HMBzoFCMAq2aBHQFRNp9Mz1ZvoXXcI1lk1180qcUM/ovXbDfPcXsUveTP1
tGzcAi2jV19h13iwJKkyv/RLmcusdsi8YunbvWGFAF5GaagYQo7Y1F6UaBQnYJTM
523AMgpPQtsKm9o/w9WdgXkgWhgkhZEeqUS3m5xNey1nLu9iMvq9M/iXnGz4sg6Q
```

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

2Y+GqZ+yAvNWjRRou3zSE7Bzg28MI4sAAwYH/2D71Xc5HPDgu87WnBFgmp8MpSr8
QnSs0wwPg3xEullGEocolSb2c0ctuSyeVnCttJMzkukL9TqyF4s/6XRstWirSWav
JxRLKH6Zjo/FaKsshYKf8gBkAaddvpl3p00gmUYbqmpQ3xDEYlhCeieXS5MkockQ
1sj2xYdB1x00ExzfiCiscUKjUFy+mdzUsUutafuZ+gbHog1CN/ccZCkxcBa5IFCH
ORrNjq9pYWlrxsEn6ApsG7JJBm2besW1PkdEoxak74z1senh36m5jQvVjA3U4xq1
wwylxadmmJaJHzeiLfb7G1ZRjZTsB7fyYxqDzMVul6o9BSwO/1XsIANv1uuITAQY
EQIADAUCOe70kgUJA8JnAAAKCRCoTtronIAKyksiAJsFB3/77SkH3J1YOGRee10J
0JdGwACeKTttgeVFPFB+iGJdiwQlXasOfuXyITAQYEQIADAUCPGqpWQUJCgCCxwAK
CRCoTtronIAKyofBAKCSZM2UFyta/fe9WgITK9I5hbxxTQCfX+0ar2CZmSknn3cc
SPihnl+OBNyZAQ0DNuEtBAAAAQgAoCRcd7SVZEFcumffYewfLTcXQjhKz0ahzxp
omuF+HIyU4AGq+SU8sTZ/1SsjhdzrSAfv1lETACA+3SmLr5KV40Us1w0UC64cwt
A46xowVq1vMlH2Lib+V/qr3b1hE67nMHjysECVx9Ob4gFuKNoR2eqnAaJvjnAT8J
/LoUC20EdCHUqn6v+M9t/WZgC+WNR8cq69uDy3YQhDP/nIan6fm2uf2kSV9A7Zx
GrswWl/WX5Q/sQqMWaU6r4az98X3z90/cN+eJJ3vwtA+rm+nxEvyeV+jaLuOQBDf
ebh/XA4FZ35xmi+spdiVeJH4F/ubaGlmj7+wDOF3suYAPSXT2QAFebQ1U3VTRSBT
ZWN1cml0eSBUZWFtIDxzZWN1cml0eUBzdXN1LmRlPokBFQMFEDbhLUfkWLKHsco8
RQEBVw4H/1vIdiOLX/7hdzYaG9crQVIk3QwaB5eBbjvLEMvuCZHiY2COUg5QdmPQ
8SlWNZ6k4nu1BLcv2g/pymPUWP9fG4tuSn1UJDrWGM3nhyhAC9iudP2u1YQY37Gb
B6NPVaZiYMnEb4QYFcv5c/r2ghSXUTYk7etd6SW6WCOpEqizhx1cqDKNZnsI/1X
11pFcO2N7rc6byDBJ1T+cK+F1Ehan9XBt/shryJmv04nli5CXQMEbiqYYMOu8iaA
8AWRgXPCWqhyGhcVD3LRhUJXjUOdH4ZiHCXaoF3zVPxpeGKEQY8iBrDeDyB3wHmj
qY9WCX6cmogGQRgYG6yJqDalLqrD0dmJARUDBRA24S0Ed7LmAD0109kBAW04B/4p
WH3f1vQn3i6/+SmDjGzUu2GWGq6Fsdwo2hVM2ym6CILEow/K9JfhdwGvY8LRxWR
hn09j2IJ9P7H1Yz3qDf10AX6V7YILHtchKT1dcngCkTLMdGc4rs1iAA13f089sRC
BafGPGKv2DQjHfR1Lfrtbf0P7c09Tkej1MP8HtQMW9hPkBYeXcwbCjdrVGFOzqx+
AvvJDdT6a+oyRMTFlvmZ83UV5pgoyimgjhWnM1V4bFBYjPrtWMkdXJSUXbR6Q7Pi
RZWCzGRzwbaxqpl3rK/YTCphOLwEMB27B4/fcqtBzgoMOiaZA0M5fF0o54KgRIhC
zinsSx2OrWgvSiLEXXYKiEYEEBECAAYFAjseYcMACgkQnkDjEAAKq6ROVACgjhDM
/3KM+iFjs5QXsnd4oFPOnbkAnjYGalJ3em+bmV2aiCdYXdOuGn4ZiQCVawUQN7c7
whaQN/70/JIVAQEB+QP/cYblsAmPxxSFiaHWB+MiUNw8B6ozBLK0QcMQ2YcL6+Vl
D+nSZP20+Ja2nfiKjnibCv5ss83yXoHkYk2Rsa8foz6Y7tHwuPiccvqnIC/c9Cvz
dbIsdxpfsi0qWPfvX/jLMpXqqnPjdIZErgxpwujas1n9016PuXA8K3MJwVjCqSKI
RgQQEQIABgUCOhpCpAAKCRDHUqoysN/3gCt7AJ9adNQMbma1iSYcbhtgvx9ByLP1
DgCfZ5Wj+f7cnYpFZI6GkAyyyczG09sE=
=LRKC

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

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

Version: GnuPG v1.2.4 (GNU/Linux)

iQEVAwUBQh32yHey5gA9JdPZAQGLMgf/VJNvZRkqx6bFLXihg/oXuCsPaE9vgJBT
DaSbxpVx0v+goK+etByCiN70NZWseqOpBYZOBnJTGbIu4VYGNiZZ6CFVHlzZIGkv

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

VTD+1QBQoK5M3aQ88RSbYpmtb6fPbOH+nJ2sIEKaX0JJ8iZp4v87KRTTanmN7tRf
qSKCwrNkMSuMQ6pD4dfTasHk3AdnBJfvMVa0alfyuqvXoLu8wlUYf+eJQvzk+24v
iqi+Afl/+pVM7Orpvj3yg8L64gJRh+52iHpnL8GU//S7cTGYIkc/HT1KAy9Ecw25
EBuwdBRqd3Inj8D5l6csb0ptQZ7H0ktrbhpVKNJOUYfH45FL4se6tg==
=LJ7l

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

--

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

---

> [Linux Reviews](#) > [News and headlines](#) > [2005 News archive](#) > [March](#) >  
Mail server administrators should seriously consider upgrading their  
servers