

Full-Disclosure: [Full-Disclosure] SUSE Security Announcement: gpg (SuSE-SA:2003:048)

[Full-Disclosure] SUSE Security Announcement: gpg (SuSE-SA:2003:048)

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2003-12/0116.html>

From: Roman Drahtmueller (*draht_at_suse.de*)

Date: 12/03/03

To: full-disclosure@lists.netsys.com

Date: Wed, 3 Dec 2003 15:22:23 +0100 (MET)

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

SUSE Security Announcement

Package: gpg

Announcement-ID: SuSE-SA:2003:048

Date: Wednesday, December 3rd 2003 15:15 MET

Affected products: 7.3, 8.0, 8.1, 8.2, 9.0

SuSE Linux Enterprise Server 7, 8

SuSE Linux Database Server,

SuSE eMail Server III, 3.1

SuSE Linux Firewall on CD/Admin host

SuSE Linux Connectivity Server

SuSE Linux Office Server

SuSE Linux Desktop 1.0

SuSE Linux School Server

SuSE Linux Standard Server 8

Vulnerability Type: cryptographic compromise, remote cmd execution

Severity (1-10): 5

SUSE default package: yes

Cross References: CAN-2003-0971

<http://www.gnupg.org/>

<http://lists.gnupg.org/pipermail/gnupg-announce/2003q4/000276.html>

Content of this advisory:

- 1) security vulnerability resolved: gpg
problem description, discussion, solution and upgrade information
 - 2) pending vulnerabilities, solutions, workarounds:
 - kernel
 - 3) standard appendix (further information)
-

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

The gnupg (the SUSE package is named gpg) package is the most widely used software for cryptographic encryption/decryption of data.

Two independent errors have been found in gpg (GnuPG) packages as shipped with SUSE products:

- A) A format string error in the client code that does key retrieval from a (public) key server
- B) A cryptographic error in gpg that results in a compromise of a cryptographic keypair if ElGamal signing keys have been used for generating the key.

A)

There exists a format string error in the client code for key retrieval from a keyserver. gpg-1.2.x version packages are affected by this vulnerability.

The format string error can be used by an attacker performing a man-in-the-middle-attack between you and your keyserver, or by a compromised keyserver. The result is a crash of gpg or a potential execution of arbitrary code provided by the attacker, if the keyserver is used for key retrieval at the time of the attack.

B)

Werner Koch, the author of the gpg package, has publicly announced a weakness in gpg that has been reported to him by Phong Nguyen: ElGamal signing keys can be attacked within seconds to reveal the private key of the keypair. It is strongly advised that ElGamal signing keys should be revoked immediately. Only ElGamal keys are affected, other types are not vulnerable.

To find out if you are using an ElGamal signing key, list your public keys using the command

```
gpg --list-keys your_keyid
```

Example:

```
$ gpg --list-keys build@suse.de
pub 1024D/9C800ACA 2000-10-19 SuSE Package Signing Key <build@suse.de>
sub 2048g/8495160C 2000-10-19 [expires: 2006-02-12]
$
```

If your key lists a capital "G" after the key's length (like in pub 1536G/...), then your key is vulnerable. A small letter "g" after the key length does NOT indicate any problem.

ElGamal keys can be used for primary keys as well as for subkeys. In the case where only a subkey is an ElGamal key, it is sufficient to revoke this specific subkey.

To revoke a key, generate a revocation certificate using the following command:

```
gpg --gen-revoke your_keyid > revocation_certificate.pgp
```

Then, the revocation certificate must be imported into your keyring:

```
gpg --import < revocation_certificate.pgp
```

As your last action, send the key with its revocation certificate to the key servers that know your key:

```
gpg --keyserver wwwkeys.eu.gpg.net --send-keys your_keyid
```

ElGamal keys can only be generated by gpg if a special option (`--expert`) has been used to reveal "expert" options, and if a warning has been ignored after your choice to use ElGamal keys. Such keys are rare (Werner Koch reports 848 primary ElGamal signing keys and 324 vulnerable subkeys on the key servers.). Therefore, we expect that only experienced users of gpg may be vulnerable to the ElGamal signing key error.

UPDATES:

The nature of the ElGamal error implies that a possible compromise was made possible with the generation of the key in the past already. There is no way that an update package can prevent the compromise. However, the update packages that we provide prevent the use of ElGamal signing keys for key generation once the packages are installed.

SUSE Linux 8.1 and before contain a gpg package of version 1.0.x (vulnerable to the ElGamal signing key bug only), a version of 1.2.x has been shipped with SUSE Linux 8.2 and 9.0 (vulnerable to both errors). We provide update packages that fix both vulnerabilities, meaning that only the packages affected by both vulnerabilities are being updated. For this reason, there are only update packages for SuSE Linux 8.2 and SUSE LINUX 9.0 available for download.

Important Note:

A proper installation of the gpg update package is critical for future updates on your system. The gpg program is being used by YaST Online Update (YOU) to verify the authenticity of your update package. A failure of a signature verification will result in a failure of the installation of update packages.

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

Full-Disclosure: [Full-Disclosure] SUSE Security Announcement: gpg (SuSE-SA:2003:048)

are being offered to install from the maintenance web.

Intel i386 Platform:

SuSE-9.0:

<ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/i586/gpg-1.2.2-121.i586.rpm>
3f3513f61408128b5a95bd251540200f

patch rpm(s):

<ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/i586/gpg-1.2.2-121.i586.patch.rpm>
227002b89a49cf3581fb1fb4c185e725

source rpm(s):

<ftp://ftp.suse.com/pub/suse/i386/update/9.0/rpm/src/gpg-1.2.2-121.src.rpm>
d3bb8845401d5e707a5da830ab209993

SuSE-8.2:

<ftp://ftp.suse.com/pub/suse/i386/update/8.2/rpm/i586/gpg-1.2.2rc1-98.i586.rpm>
ff54dbcb36cf741f108bdd48d5496e5d

patch rpm(s):

<ftp://ftp.suse.com/pub/suse/i386/update/8.2/rpm/i586/gpg-1.2.2rc1-98.i586.patch.rpm>
0efef8f33670349639fa5c25b3c5f3a3

source rpm(s):

<ftp://ftp.suse.com/pub/suse/i386/update/8.2/rpm/src/gpg-1.2.2rc1-98.src.rpm>
13ee0ff9bb2137365ab91f32324a4114

Opteron x86_64 Platform:

SuSE-9.0:

ftp://ftp.suse.com/pub/suse/x86_64/update/9.0/rpm/x86_64/gpg-1.2.2-117.x86_64.rpm
a1679f36e00347a1adf53e2209245274

patch rpm(s):

ftp://ftp.suse.com/pub/suse/x86_64/update/9.0/rpm/x86_64/gpg-1.2.2-117.x86_64.patch.rpm
f3002d4cea60bb0acea1e8bea89d46c9

source rpm(s):

ftp://ftp.suse.com/pub/suse/x86_64/update/9.0/rpm/src/gpg-1.2.2-117.src.rpm
50e58f6853dcd5523172cb4c07a63d89

2) Pending vulnerabilities in SUSE Distributions and Workarounds:

– kernel: brk() vulnerability

All SUSE Linux kernels (except for the SUSE Linux Enterprise Server 8) are vulnerable to a privilege escalation vulnerability that can be exploited by an attacker who has local shell access to your system.

We are in the process of testing the update packages for all of our products. The packages are expected to be released within hours and are being published as they are ready.

Please follow the guidelines in the announcement about the kernel that follows this announcement.

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)

Full-Disclosure: [Full-Disclosure] SUSE Security Announcement: gpg (SuSE-SA:2003:048)

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
```

[Full-Disclosure] SUSE Security Announcement: gpg (SuSE-SA:2003:048)

myW/xC1sBbDkDUIBSx5oej73XCZgnj/inphRqGpsb+1nKFvF+rQoU3VTRSBQYWNr
YWdlIFNpZ25pbmcgS2V5IDxidWlsZEBzdXNlMlRlPohcBBMRAgAcBQI57vSBBQkD
wmcABAsKAwQDFQMCAxYCAQIXgAAKCRCoTtronIAKyl8sAJ98BgD40zw0GHJHlf6d
NfnwI2PAsgCgjH1+PnYEI7TFjtZsqhezX7vZvYcIRgQQEQIABgUCOnBeUgAKCRCE
QOMQAAqrpNzOAKCL512FZvv4VZx94TpbA9lxyoAejACeOO1HIbActAevk5MUBhNe
LZa/qM2JARUDBRA6cGBvd7LmAD0l09kBATWnB/9An5vfiUUE1VQnt+T/EYkIES3t
XXaJjP9pHMa4fzFa8jPVtv5UBHGee3XoUNdVwM2OgSEISZxbzdXGnqllcT08TzBU
D9i579uifkLlsnr35SJDZ6ram51/CWOnnaVhUzneOA9gTPSr+/ft3WeVnwJiQCQ3
0kNLWVXWATMnsnT486eAOIT6UNBPYQLpUprF5Yryk23pQUPAgJENDEqeU6iIO9Ot
1ZPtB0lniw+/xCi13D360o1tZDYOp0hHHJN3D3EN8C1yPqZd5CvvnYvB6bWBIPW
cRgdn2DUVMmpU661jwqGIRz1F84JG/xe4jGuzgpJt9IXSzyohEJB6XG5+D0BiFOE
ExECAB0FAjxqqTQFCQoAgrMFCwcKAwQDFQMCAxYCAQIXgAAKCRCoTtronIAKyp1f
AJ9dR7saz2KPNwD3U+fy/0BDKXrYGACfbJ8fQcJqCBQxeHvt9yMPDVq0B0W5Ag0E
Oe70khAIAISR0E3ozF/la+oNaRwxHLrCet30NgnXRROyhPaJB/Tu1FQokn2/Qld/
HZnh3TwhBIw1FqrhWBJ7491iAjLR9uPbdWJrn+A7t8kSkPaF3Z/6kyc5a8fas44h
t5h+6HMBzoFCMAq2aBHQFRNp9Mz1ZvoXXc11k118OqcUM/ovXbDfPcXsUvETPT
tGzcAi2jV19hl3iwJKkyv/RLmcusdsi8YunbvWGFAF5GaagYQo7YIF6UaBQnYJTM
523AMgpPQtsKm9o/w9WdgXkgWhgkhZEEqUS3m5xNey1nLu9iMvq9M/iXnGz4sg6Q
2Y+GqZ+yAvNWjRRou3zSE7Bzg28MI4sAAwYH/2D71Xc5HPDgu87WnBFgmp8MpSr8
QnSs0wwPg3xEullGEocolSb2c0ctuSyeVnCttJMzkukL9TqyF4s/6XRstWirSWaw
JxRLKH6Zjo/FaKsshYKf8gBkAaddvpl3pO0gmUYbqmpQ3xDEYlhCeieXS5MkockQ
1sj2xYdB1xO0ExzfiCiscUKjUFy+mdzUsUutafuZ+gbHog1CN/ccZckxcBa5IFCH
ORrNjq9pYWlrxsEn6ApsG7JJbM2besW1PkdEoxak74z1senh36m5jQvVjA3U4xq1
wwylxadmmJaJHzeiLfb7G1ZRjZTsB7fyYxqDzMVul6o9BSwO/1XsIAAnV1uuITAQY
EQIADAUCOe70kgUJA8JnAAAKCRCoTtronIAKysIAJsFB3/77SkH3JIYOGreE1Ol
0JdGwACeKtTtgeVPFB+iGJdiwQlxasOfuXyITAQYEQIADAUCPGqpWQUJcGCcxwAK
CRCoTtronIAKyofBAKCSZM2UFyta/fe9WgITK9I5hbxxTQCfX+0ar2CZmSknn3co
SPihnl+OBnyZAQ0DNuEtBAAAAQgAoCRcd7SVZEFcumffyEwflTcXQjhKzOahzxp
omuF+HIyU4AGq+SU8sTZ/1SsjhdzrSafv1IETACA+3SmLr5KV40Us1w0UC64cwt
A46xowVq1vMIH2Lib+V/qr3b1hE67nMHjysECVx9Ob4gFuKNoR2eqnAaJvjnAT8J
/LoUC20EdCHUqn6v+M9t/WZgC+WNR8cq69uDy3YQhDP/nIAn6fm2uf2kSV9A7Zx
EGrwsWl/WX5Q/sQqMwU6r4az98X3z90/cN+eJJ3vwtA+rm+nxEvyeV+jaLuOQBdf
ebh/XA4FZ35xmi+spdiVeJH4F/ubaGlmj7+wDOF3suYAPSXT2QAFebQIU3VTRSBT
ZWN1cml0eSBUZWFtIDxzZWN1cml0eUBzdXNlMlRlPohcBFQMFEDbhLUfkWLKHsco8
RQEBVw4H/1vIdiOLX/7hdzYaG9crQVik3QwaB5eBbjvLEMvuCZHiY2COUg5QdmPQ
8SIWNZ6k4nu1BLcv2g/pymPUWP9fG4tuSnIUDrWGM3nhyhAC9iudP2u1YQY37Gb
B6NPVaZiYmNEb4YFfcqv5c/r2ghSXUTYk7etd6SW6WCOPEqizhx1cqDKNZnsI/1X
11pFcO2N7rc6byDBJ1T+cK+F1Ehan9XBt/shryJmv04nli5CXQMEbiqYYMOu8iaA
8AWRgXPCWqhyGhcVD3LRhUJXjUOdH4ZiHCXaoF3zVPxpeGKEQY8iBrDeDyB3wHmj
qY9WCX6cmogGQRgYG6yJqDalLqrDODmJARUDBRA24S0Ed7LmAD0l09kBAW04B/4p
WH3f1vQn3i6/+SmDjGzUu2GWGq6Fsdwo2hVM2ym6CILEow/K9JfhdwGvY8LRxWRL
hn09j2IJ9P7H1Yz3qDf10AX6V7YILHtchKT1dcngCkTLMdGc4rs1iAA13f089sRG
BafGPGKv2DQjHfR1Lfrtbf0P7c09Tkej1MP8HtQMW9hPkBYeXcwbCjdrVGFozqx+
AvvJdDt6a+oyRMTFlvmZ83UV5pgoyimgjhWnM1V4bFBYjPrtWMkdXJSUXbR6Q7Pi
RZWCzGRzwbaxqpl3rK/YTCphOLwEMB27B4/fcqtBzgoMOiaZA0M5fFoo54KgRIh0
zinsSx2OrWgvSiLEXXYKiEYEEBECAAYFAjseYcMACgkQnkDjEAAKq6ROVACgjhDM
/3KM+iFjs5QXsnd4oFPOnbkAnjYGa1J3em+bmV2aiCdYXdOuGn4ZiQCVaWUQN7c7
whaQN/7O/JIVAQEB+QP/cYblSAmPXxSFiaHWB+MiUNw8B6ozBLK0QcMQ2YcL6+V1
D+nSZP20+Ja2nfiKjnbCv5ss83yXoHkYk2Rsa8fz6Y7tHwuPiccvqnlc/c9Cvz
dbIsdxpfsi0qWPfvXjLMPxqqnPjdIZErgxpWujas1n9016PuXA8K3MJwVjCqSKI
RgQQEQIABgUCOHPcPAAKCRDHUqoysN/3gCt7AJ9adNQMbmA1iSYcbhtgvx9ByLPI

Full-Disclosure: [Full-Disclosure] SUSE Security Announcement: gpg (SuSE-SA:2003:048)

DgCfZ5Wj+f7cnYpFZI6GkAyyczG09sE=
=LRKC
-----END PGP PUBLIC KEY BLOCK-----

Roman Drahtmueller,
SUSE Security.

--
--

| Roman Drahtmueller <draht@suse.de> // "You don't need eyes to see, |
| SUSE Linux AG – Security Phone: // you need vision!"
| Nuernberg, Germany +49-911-740530 // Maxi Jazz, Faithless |

--

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

Version: GnuPG v1.0.7 (GNU/Linux)

iQEVAwUBP83wP3ey5gA9JdPZAQGZcgf8CTme9Nl+vX4h+eN2E+r1XQuU1tdlEq6g
gRXIf7psQ2mwCgsuCjSc25e60ikKi1kCpEY95vId6SwlkKfw9W10kZfvndc4dvjl
4X80dO60es4p7IIZJn643MIrpjH3EdffVaPnj7SFHaYqCSnHvm6QFuToZ0UD2bzo
nLZAGJoPGef4d9ocX/yqC76Wmqc5vMiC2mt8BQBwCtiHOHjYPZILCryrX5x+VZcK
8YENI3IzZiEEpHV6UgWwBOzujq+l/1bCPkLBRRoze2MukF/7HW6USVxFIsJXy4qJ
WyMqyy3EACtORun6+FjqZQmGd8JJYZLqK+UpVs4T8FzV+vbj6KK/Tw==
=McN2

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

Full-Disclosure – We believe in it.

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