CERT Advisory CA-2000-09 Flaw in PGP 5.0 Key Generation

Original release date: May 30, 2000
Last Revised: --
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- UNIX systems having a */dev/random* device running any version of PGP 5.0, including U.S. Commercial, U.S. Freeware, and International versions
- Keys created non-interactively on such a system
- Documents encrypted with such a key
- Signatures generated with such a key

Overview

Under certain circumstances, PGP v5.0 generates keys that are not sufficiently random, which may allow an attacker to predict keys and, hence, recover information encrypted with that key.

I. Description

In order to generate cryptographically secure keys, PGP (and other products) need to use random numbers as part of the input to the key generation process. Generating truly random numbers is a difficult problem. PGP has traditionally solved that problem by prompting the user to type some random characters or to move the mouse in a random manner, measuring the time between keystrokes and using this as a source of random data. Additionally, PGP uses a file (usually called *randseed.bin*) as a source of randomness. However, PGP also provides the ability to generate keys non-interactively (useful, for example, if you need to generate a large number of keys simultaneously or provide a script to generate a key). When generating keys non-interactively, PGP needs a source of random numbers; on some systems PGP v5.0 uses the */dev/random* device to provide the required random numbers.

PGP v5.0, including U.S. Commercial, U.S. Freeware, and International versions, contains a flaw in reading the information provided by */dev/random.* This is not a flaw in */dev/random* but instead is the result of a flaw in how PGP processes the information returned from */dev/random.* Thus, when a key is generated non-interactively using a command such as

> **pgpk -g** <*DSS or RSA*> <*key-length*> <*user-id*> <*timeout*> <*pass-phrase*>

it does not contain sufficient randomness to prevent an attacker from guessing the key. If such a command were issued on a system with no available *rand seed.bin* file, then the resulting key may be predictable.

This problem was discovered and analyzed by Germano Caronni <gec@acm.org>, and verified by Thomas Roessler <roessler@guug.de> and Marcel Waldvogel <mwa@arl.wustl.edu>. A copy of their analysis can be found at

> http://www.securityfocus.com/templates/ archive.pike?list=1&msg=20000523141323.A28431@olymp.org

II. Impact

> Keys produced non-interactively with PGP v5.0 on a system with a */dev/random* device may be predictable, especially those produced in an environment without a pre-existing *randseed.bin* file.
>
> Documents encrypted with a vulnerable key may recoverable by an attacker. Additionally, an attacker may be able to forge a digital signature corresponding to a vulnerable key.
>
> Signatures produced using a vulnerable key, including signatures in certificates, may be untrustworthy.

III. Solution

> If your PGP key was generated non-interactively using any version of PGP v5.0 on a system with a */dev/random* device, you may wish to revoke it.
>
> Documents encrypted with a predictable key may need to be re-encrypted with a non-vulnerable key, if your particular circumstances warrant it; that is, if the information still needs to be encrypted.
>
> You may need to resign documents signed with a vulnerable key if your circumstances warrant it.

Appendix A Vendor Information

Network Associates

Network Associates Security Advisory
Date: May 30, 2000
Author: PGP Engineering

Background:

A security issue has been discovered in the following PGP products:

- PGP 5.0 for Linux, US Commercial and Freeware editions
- PGP 5.0 for Linux, Source code book (basis for PGP 5.0i for Linux)

The following PGP products are NOT affected by this issue:

- PGP 1.x products
- PGP 2.x products
- PGP 4.x products
- All other PGP 5.x products
- PGP 6.x products
- PGP 7.x products

Synopsis:

During a recent review of our published PGP 5.0 for Linux source code, researchers discovered that under specific, rare circumstances PGP 5.0 for Linux will generate weak, predictable public/private keypairs. These keys can only be created under the following circumstances:

- Keys are generated using PGP's command line option for unattended batch key generation, with no user interaction for entropy (random data) collection
- No keys were generated interactively on this system previously (e.g., a PGP random seed file is not present on this system prior to unattended batch key generation)
- PGP is able to access the UNIX /dev/random service to gather entropy during unattended batch key generation

PGP 5.0 for Linux does not process the data read from /dev/random appropriately, and therefore does not gather enough entropy required to generate strong public/private keypairs. This issue affects both RSA and Diffie-Hellman public/private keypairs, regardless of keysize. Network Associates has verified that this issue does not exist in any other version of PGP.

Solution:

Users who generated keys in the manner described above are strongly urged to do the following:

- Revoke and no longer use keys suspected to have this problem
- Generate new public/private keypairs with entropy collected from users' typing and/or mouse movements
- Re-encrypt any data with the newly generated keypairs that is currently encrypted with keys suspected to have this problem
- Re-sign any data with the newly generated keypairs, if required

Users are also urged to upgrade to the latest releases of PGP, as PGP 5.0 products have not been officially supported by Network Associates since early 1999, or distributed by Network Associates since June 1998.

Additional Information:

US commercial and freeware versions of PGP 5.0 for Linux were released in September 1997 by PGP, Inc., a company founded by Phil Zimmermann. Source code for the PGP 5.0 product family was published in September 1997. PGP, Inc. was acquired by Network Associates in December 1997.

Acknowledgements:

PGP appreciates the efforts of Germano Caronni, Thomas Roessler and Marcel Waldvogel in identifying this issue and bringing it to our attention.

A
pgp signed version of this statement is also available at

http://www.cert.org/advisories/CA-2000-09/pgp.asc

The CERT Coordination Center thanks Germano Caronni, Thomas Roessler, and Marcel Waldvogel for initially discovering and reporting this vulnerability, and for their help in developing this advisory. Additionally we thank Brett Thomas for his insights.

Shawn Hernan was the primary author of this document.

Revision History

```
May 30, 2000:  initial release
```