

The Debain SSL Fiasco

Radu Ciorba radu@devrandom.ro

March 15, 2016

OpenSSL

- Started in 1998, as a fork of SSLeay
- Focused on being a Free (as in free speech) SSL/TLS library
- Volunteer effort
- SSH, HTTPS

Debian

- First announced August 1993
- Focused on being a Free (as in free speech) distribution
- Volunteer effort

Entropy

- Crypto requires random numbers
- Computers are quite deterministic
- Use low entropy data and run it through a hash function
- `/dev/random`; Windows CryptoAPI

OpenSSL PRNG

- `RAND_add(const void *buf, int num, double entropy);`

```
// a simplification of what's going on
char buf[100];
fd = open("/dev/random", O_RDONLY);
n = read(fd, buf, sizeof buf);
RAND_add(buf, sizeof buf, n);
```

A bit of added value

Subject: Random number generator, uninitialised data and valgrind.
Date: 2006-05-01 19:14:00

...

The code in question that has the problem are the following 2 pieces of code in `crypto/rand/md_rand.c`:

247:

```
MD\_update(&m,buf,j);
```

467:

```
#ifndef PURIFY
```

```
MD\_update(&m,buf,j); /* purify complains */
```

```
#endif
```

Implications of that change

- Basically the PID is the only source of entropy
- 15 bits, a whopping 32768 for each architecture

DILBERT By SCOTT ADAMS



Timeline

- 2 May 16:34:53 2006 UTC
- 13 May 2008 DSA-1571-1 – predictable PRNG
- Debian 4, Ubuntu 7.04/7.10/8.04 LTS

What does it mean

- ssh-keygen
- openssl genrsa -out /domain.com.ssl/domain.com.key 2048
- Diffie Hellman Key Exchange

Pwnie awards 2008

And the Mass Ownage Award goes to:

Pwnie awards 2008

And the Mass Ownage Award goes to:

An unbelievable number of WordPress vulnerabilities (CVE-2008-*)

Discovered by: everybody who cared to look

Pwnie awards 2008

And the Mass Ownage Award goes to:

An unbelievable number of WordPress vulnerabilities (CVE-2008-*)

Discovered by: everybody who cared to look

New category was introduced: Most Epic Fail

Debian for shipping a vulnerable OpenSSL for almost 2 years.

Thank you

Read more about this:

- <http://goo.gl/DmPyja> the actual commit
- <http://research.swtch.com/openssl> very good analysis