



Products

Services

Publications

Resources

What's new

Follow @Openwall on Twitter for new release announcements and other news

[<prev] [next] [<thread-prev] [thread-next] [day] [month] [year] [list]

Message-ID: <1327625373.3101.62.camel@mdlinux>

Date: Thu, 26 Jan 2012 19:49:33 -0500

From: Marc Deslauriers <marc.deslauriers@...onical.com>

To: oss-security@...ts.openwall.com

Subject: Re: CVE Request: Debian (others?) openssh-server:

Forced Command handling leaks private information to ssh clients

On Thu, 2012-01-26 at 16:22 -0700, Kurt Seifried wrote:

> On 01/26/2012 04:19 PM, Kurt Seifried wrote:

> > <http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=657445>

> >

> > =====

> >

> > From: Bjoern Buerger <bbu@...gutronix.de>

> > To: Debian Bug Tracking System <submit@...s.debian.org>

> > Subject: openssh-server: Forced Command handling leaks private

> > information to ssh

> > clients

> > Date: Thu, 26 Jan 2012 11:46:18 +0100

> >

> > Package: openssh-server

> > Version: 1:5.5pl-6+squeezel

> > Severity: normal

> >

> >

> > The handling of multiple forced commands in ~/.ssh/authorized key leaks

> > information about other configured forced commands to the user. This

> > affects tools like gitolite, which makes heavy use of forced commands

> > (For gitolite, this bug means: A user can obtain some or all usernames

> > with access to the same gitolite setup by just using the verbose

> > switch of his ssh client, which is a really nasty thing).

> >

> > Example:

> >

> > User "bbu" on machine "ptx" has three configured forced commands for

> > keys test{1,2,3}_rsa.pub:

> >

> > command="/usr/bin/first_command" ssh-rsa [...third_key...]

> > command="/usr/bin/second_command" ssh-rsa [...second_key...]

> > command="/usr/bin/third_command" ssh-rsa [...third_key...]

> >

> > Now, if the user of test1_rsa.pub uses the "-v" switch of

> > his ssh client, he gets just his command:

> >

> > foo@bar:~/ssh_debug\$ ssh -i test1_rsa -v bbu@ptx 2>&1 | grep Forced\

> > command

> > debug1: Remote: Forced command: /usr/bin/first_command

> > debug1: Remote: Forced command: /usr/bin/first_command

> >

> > but the user of test2_rsa.pub sees two commands:

> >

> > foo@bar:~/ssh_debug\$ ssh -i test2_rsa -v bbu@ptx 2>&1 | grep Forced\

> > command

> > debug1: Remote: Forced command: /usr/bin/first_command

> > debug1: Remote: Forced command: /usr/bin/second_command

> > debug1: Remote: Forced command: /usr/bin/first_command

> > debug1: Remote: Forced command: /usr/bin/second_command

> >

> > and for user of test3_rsa.pub:

> >

> > bbu@...ra:~/ssh_debug\$ ssh -i test3_rsa -v bbu@ptx 2>&1 | grep Forced\

> > command

> > debug1: Remote: Forced command: /usr/bin/first_command

> > debug1: Remote: Forced command: /usr/bin/second_command

> > debug1: Remote: Forced command: /usr/bin/third_command

```
> > debug1: Remote: Forced command: /usr/bin/first_command
> > debug1: Remote: Forced command: /usr/bin/second_command
> > debug1: Remote: Forced command: /usr/bin/third_command
> > =====
> >
> > I have confirmed that this works exactly as advertised on Debian 6. I
> > have confirmed that RHEL/Fedora are not affected (you only get shown the
> > command for your specific SSH key).
> >
> > So Debian is definitely affected, but I am concerned others may be as
> > well (is this Debian specific or does it affect all users of that
> > version of OpenSSH?). I suggest you test this on your own distributions
> > as well.
>
> Please use CVE-2012-0814 for this issue. Also please let me know if
> other Linux distributions are affected!
>
>
```

Looks like this (I haven't tried...):

<http://www.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/auth-options.c.diff?r1=1.53;r2=1.54>

Marc.

--

Marc Deslauriers
Ubuntu Security Engineer | <http://www.ubuntu.com/>
Canonical Ltd. | <http://www.canonical.com/>

[Powered by blists - more mailing lists](#)

Please check out the [Open Source Software Security Wiki](#), which is counterpart to this [mailing list](#).

Confused about [mailing lists](#) and their use? [Read about mailing lists on Wikipedia](#) and check out these [guidelines on proper formatting of your messages](#).