

Re: OT: security of make as authorized_keys command

Source: <http://linux.derkeiler.com/Mailing-Lists/Fedora/2007-12/msg04383.html>

- *From:* "Mikkel L. Ellertson" <mikkel@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 31 Dec 2007 12:20:55 -0600
-

Dave Burns wrote:

I should probably ask this on an ssh oriented list, but I thought I'd try my luck here first.

I want to do some remote commands securely. I put a key in my .ssh/authorized_keys file like so:

```
command="/usr/bin/make $$SSH_ORIGINAL_COMMAND" ssh-rsa  
AAAAB3NzaC1[etc.etc.]
```

so I can invoke make targets like so:

```
ssh username@host target
```

Assuming the bad guys never get my key, I am fine, even though it is passwordless.

What if a bad guy does get my key? Then I see three possible problems:

- 1) somehow use make's -F switch in ssh command to change Makefiles?
- 2) stack overflow of make or ssh?
- 3) Somehow put extra command after make target using ';' or something?

And obviously the bad guy can invoke any of the targets in my makefile, but I've made them pretty innocuous.

So, should I seriously worry about any of these potential problems? Any other holes I haven't thought of?

The motivation for all this is some cron jobs I want to run, obviously calls for a passwordless ssh key, but I want to put some limits on it.

Thanks,
Dave

Re: OT: security of make as authorized_keys command

Instead of running make directly, run a script that does some checking on what is supplied. You could limit the directories that make could be run in, strip out any extra command, etc. (Search the line for a ; , then log and discard the command if it is found.) You could even disable the key if you get an invalid command.

As added security, you can limit the IP address that the key is valid from, so the key would only be useful from a specific network.

Mikkel

—

Do not meddle in the affairs of dragons,
for thou art crunchy and taste good with Ketchup!

Attachment: signature.asc

Description: OpenPGP digital signature

—

fedora-list mailing list

fedora-list@xxxxxxxxxx

To unsubscribe: <https://www.redhat.com/mailman/listinfo/fedora-list>