

Re: Authentication failed suddenly

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2002-10/2177.html>

From: Per Hedeland (per@hedeland.org)

Date: 09/21/02

From: per@hedeland.org (Per Hedeland)
Date: Sat, 21 Sep 2002 20:39:25 +0000 (UTC)

In article <GO_i9.5992\$ep5.2939@nwrddc01.gnilink.net> "Nico Kadel-Garcia" <nkadel@bellatlantic.net> writes:

>
> "Per Hedeland" <per@hedeland.org> wrote in message
> news:amhmda\$2j1o\$2@hedeland.org...
>> You keep saying things like this, but perhaps you could be a bit more
>> specific? The only problem I've observed is that privilege separation
>> and compression won't function together on some platforms – as noted in
>> the documentation, i.e. this is not really a bug but a limitation of the
>> current implementation. And of course nothing forces you to use
>> privilege separation just because you run a version that has it, just
>> turn it off and you have the same functionality in this respect as the
>> 3.1p1 that you advocate. And if you turn neither privsep nor compression
>> off on such a platform, sshd dutifully prints
>
> Some kernels don't support it,

Some kernels don't support what? OpenSSH? The fact that some kernels don't support the combination of privsep and compression is prominently mentioned in the documentation.

> it doesn't compile correctly out of the box
> on a lot of platforms it used to work on (Solaris was an adventure, as was
> Tru64 with undocumented gcc version dependencies,

An "adventure" indeed – just the sort of specific technical detail I was asking for. It compiles and runs without a hitch for me on Solaris 8 (using gcc from the "Software companion CD" or whatever it's called). I don't have a Tru64 box, nor does most other people, but I wouldn't be surprised if there was no problem there either when using reasonably up-to-date development tools. I also have no problem on RH 6.x/7.x or FreeBSD 4.x, which together with OpenBSD (and I'm sure the other *BSD* are fine too) covers the vast majority of Unix systems.

> the new spec files don't
> work with older RPM versions for RedHat, it depends on a bleeding edge

comp.security.ssh: Re: Authentication failed suddenly

>version of autoconf to be able to modify the configure.ac/configure files,
>etc.),

I don't know where the RPM stuff in the distribution comes from, but the fact that it is in a 'contrib' subdirectory is a clear indication that the developers don't consider it a fundamental part of the distribution. I'm of course talking about building with the standard configure/make procedure, which works perfectly fine on RedHat. If you require RPMs, by all means stick to what your vendor provides – that's no basis for badmouthing the distribution as such.

> and it broke the available chroot tools.

Are you seriously suggesting that the developers have a responsibility to ensure that each new release is compatible with third-party patch kits?

> It's just nasty if you're
>the poor bugger who has to work out the full details for it. The enabling of
>PrivSep fails, if it's going to fail, at daemon start time,

Of course. That's the only point in time when it can be known that it will fail.

> so if you're
>installing it remotely and accidentally enable it with an inappropriate
>setup (such as compression on some platform, inappropriate sshd or
>/var/empty on other platforms, etc.), you lose your active ssh daemon unless
>you've stashed an old one and left it running on another port.

This is getting silly. If you're stupid enough to replace software that is critical for your access to a remote system without prior testing, you have no-one to blame but yourself. And of course you don't lose your active *session* unless you're using broken RedHat rc scripts that kill every instance of "sshd" in sight instead of just reading the pid file to find the daemon.

But I begin to see where your aversion is coming from – your patch kit doesn't work until you have fixed it, and through sheer incompetence you have locked yourself out of a remote system – and now you try to blame it all on OpenSSH.

>Those are the obvious failures: they're enough to keep even expert people
>away from it unless they like the bleeding edge dripping all over them.

More sweeping ramblings. Which are those "expert people" exactly? Names and references to their statements please.

>It never should have been put in the code until it had a lot more testing.
>The code is clearly not mature, which is a bad sign in a high-security tool.
>It may work well for OpenBSD, the source platform for OpenSSH, but elsewhere

Re: Authentication failed suddenly

comp.security.ssh: Re: Authentication failed suddenly

>*it should be taken out and run through a Roto-Rooter drain cleaner testing
>cycle.....*

This exactly is the kind of generic, unsubstantiated nonsense you have been posting here for several weeks now – provide specific details or stop doing it.

>*It should *FAIL* in this case, not issue a quiet error message.*

That's your opinion, I definitely disagree – the WARNING is printed as the very last thing of the 'make install', you can hardly miss it. And to be more than a warning, it would have to parse the config file to see if privsep was actually on, and make the unfounded assumption that the admin wouldn't modify the config file after installation. In fact it would be perfectly fine if this check wasn't done at all, I guess it was only put in as a hint to those that can't be bothered to read release notes and other documentation.

>*True. I'm sure they follow this group, and the failures reported here have
>been many and varied.*

So you say – I follow the group pretty closely too, and haven't seen any verified actual problems with the code reported – and my previous message provided a detailed analysis of what **has** been reported.

> *They have put 3.4p1 on the rawhide site for testing:
>you can play with that one if you like, but it has a lot of library
>dependencies, and I'd recompile from the SRPM.*

Putting things on RawHide before integrating them into a release is standard procedure for RedHat I believe – it's no indication of quality problems, rather the opposite – if there were serious problems, it wouldn't even be on RawHide.

>> *– combined with the fact that it has now been out for almost two months
>> without being "superseded". If it was chock-full of bugs like you claim,
>> I'm sure the good folks developing/maintaining OpenSSH and the portable*

^^^^^^^^^^^^^^^^^^^^

>> *version would have a bugfixed version out by now.*
^^^^^^

>*The bugs are platform compatibility bugs. Near as I can tell, they don't
>occur under OpenBSD.*

Nor on most other OSes, near as **I** can tell.

> *And they're waiting, not surprisingly, for us to find
>those bugs and fix them:*

Is this more conjecture, or do you have some basis for this claim? Of course all open-source developers hope that users will help them find bugs and report (or even fix) them – rather than rambling in public fora

comp.security.ssh: Re: Authentication failed suddenly

about how the code is not "mature" or "robust" – but that doesn't mean that they just sit back and wait rather than try things out themselves on the major OSes.

--Per Hedeland
per@hedeland.org

- *Next message:* : ["Re: openssh server doesn't connect to ssh client"](#)
- *Previous message:* [Richard E. Silverman: "Re: openssh server doesn't connect to ssh client"](#)
- *In reply to:* : ["Re: Authentication failed suddenly"](#)
- *Next in thread:* : ["Re: Authentication failed suddenly"](#)
- *Reply:* : ["Re: Authentication failed suddenly"](#)
- *Messages sorted by:* [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)