

Re: Can't login to an OS X box using ssh

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2003-02/0323.html>

From: Richard E. Silverman (slade@shore.net)

Date: 02/26/03

From: slade@shore.net (Richard E. Silverman)

Date: 26 Feb 2003 10:10:32 -0500

> (*Explanation of "debug1: sshd version <CHANGED>": one of my linux guru
> friends seemed to think that sshd giving out it's version tag was a
> security issue since a hacker could look for vulnerabilities in that
> particular version. This seemed correct to me at the time and so I
> allowed him to help me hack the sshd to display a wierd string there.
> It worked fine after I made the change and sshd is still working in
> some cases, so I don't think this is the problem. But then again, I
> could be wrong ;-)*)

Yes, you and your friend are wrong; this is your problem. The version comment string allows SSH programs to recognize specific implementations and work around known incompatibility problems. In this case, it's an issue with the DH group-exchange draft protocol extension. If you return the string to its normal state, this problem will go away.

Munging the string is not a real security win anyway, since your attacker can simply try known exploits and see if they work. In fact, since your attacker knows that you can change that string if you want and hence he can't trust it, it's probably what he's going to do anyway.

<http://www.snailbook.com/faq/version-string.auto.html>

--

Richard Silverman
slade@shore.net