

## Re: OpenSSH 3.4p1 Trouble on SCO 5.0.5?

---

*Source:* <http://unix.derkeiler.com/Newsgroups/comp.unix.sco.misc/2008-03/msg00227.html>

---

- *From:* Nico Kadel-Garcia <[nkadel@xxxxxxxxx](mailto:nkadel@xxxxxxxxx)>
  - *Date:* Sun, 23 Mar 2008 12:11:52 +0000
- 

Steve M. Fabac, Jr. wrote:

I have a client running SCO 5.0.5 with OpenSSH 3.4p1 installed.

Since SSH was installed, we have been getting hits from people on the Internet scanning port 22.

Normally they give up and go away. However, I have noticed an unusual number of scans from foreign IP addresses using valid names on the system (the names below in the block for a single source IP are the *\*only\** names logged from that IP):

Are you running an SMTP server that can be probed for valid addresses? A lot of those are common system names, as well. Someone could have gotten a valid `/etc/passwd` list by any of a number of other means, published it, and be probing them with their rootkit tools.

However, 5.0.5 is way out of date. It has no, and I mean *\*NO\** business having any direct exposure to the Internet. If you have to run services like SSH to it, it should be through an external firewall with some sort of logging, and preferably not run popular services like SSH on port 22.

Anybody have any ideas, thoughts or comments on this?

It looks like normal port scanning by crackers. Any machine exposed to the Internet will see this sort of scanning, with the caveat that the user names may be obtained from some other source (such as public email addresses off of the web) or may be from random guessing of likely first-name addresses.

.