

# Re: On why debugging OpenSSH can be so hard

---

*Source:* [http://www.derkeiler.com/Mailing-Lists/securityfocus/Secure\\_Shell/2008-07/msg00024.html](http://www.derkeiler.com/Mailing-Lists/securityfocus/Secure_Shell/2008-07/msg00024.html)

---

- *From:* Maurice Volaski <[mvolaski@xxxxxxxxxxxxx](mailto:mvolaski@xxxxxxxxxxxxx)>
  - *Date:* Wed, 9 Jul 2008 12:12:42 -0400
- 

No. He's saying that it leaks information that doesn't need to be leaked.

But this is a straw man argument.

Since nobody seems to be aware of how debugging works on OpenSSH, let me just tell you that there is a client process and a server process and they separately have debug modes. These debug modes are entirely independent from one another. And what is displayed on the server never gets near the client. The client debug mode could merely say "Login failed. Ask your admin to run in debug mode to diagnose this problem." and let it go at that. The server mode is where all the juicy details go.

Please let me know how the attacker is going to get the server into debug mode, let alone read its output?

For comparison, long long ago, there used to be different error messages when authentication failed. It would helpfully tell you that your password was wrong, or that you'd supplied the wrong username.

Great for debugging, right? Well yeah ... and it was great for enumerating the users on the box, making further attacks much simpler.

Apparently they had more diligent programmers back then; they just put the information in the wrong log file.

By the way, you might want to actually read the bug report. Nowhere is the OpenSSH programmer indicating any concern of security; he is even calling my suggestion "logspam". Then again, perhaps he's not aware of this supposedly long-debated security issue.

--

Maurice Volaski, [mvolaski@xxxxxxxxxxxxx](mailto:mvolaski@xxxxxxxxxxxxx)  
Computing Support, Rose F. Kennedy Center  
Albert Einstein College of Medicine of Yeshiva University