

## Re: OPENSSSH 3.4p1-3 on AIX 4.3.3

**Source:** [http://www.derkeiler.com/Mailing-Lists/securityfocus/Secure\\_Shell/2003-02/0086.html](http://www.derkeiler.com/Mailing-Lists/securityfocus/Secure_Shell/2003-02/0086.html)

---

**From:** Neil Martin ([Neil@Car-Part.com](mailto:Neil@Car-Part.com))

**Date:** 02/14/03

Date: Fri, 14 Feb 2003 08:17:21 -0500  
From: Neil Martin <[Neil@Car-Part.com](mailto:Neil@Car-Part.com)>  
To: Alf Nicolaysen <[Alf.Nicolaysen@de.ibm.com](mailto:Alf.Nicolaysen@de.ibm.com)>

Alf,

That parameter ReverseMapping under 3.5 should default to no, so it being commented out should be ok. There seems to some deeper issue here.

Try setting HostbasedAuthentication yes.

Neil

Alf Nicolaysen wrote:

>Hi, Neil.  
>  
>What you guessed is right. The RhostsAuthentication is set to yes and the  
>ignorerhosts is set to no. The Reversemapping was commented out in the  
>sshd\_config, I commented it in, but unfortunately without changes to the  
>result. Teh debug output from the server is exactly the same, except  
>another port (which of course I can not determine).  
>  
>The DNSLookup AND the ReverseLookup are working fine, as they are doing for  
>all other applications. But I guess you are right, ErrorMessage points to  
>that DNS-Problem which I cannot see on one of the machines.  
>  
>regards  
>  
>  
>  
>Alf Nicolaysen  
>  
>  
>Neil Martin <[Neil@Car-Part.com](mailto:Neil@Car-Part.com)> on 14.02.2003 13:47:54  
>  
>To: Alf Nicolaysen/Germany/Contr/IBM@IBMDE  
>cc:  
>Subject: Re: OPENSSSH 3.4p1-3 on AIX 4.3.3

SecurityFocus Secure Shell: Re: OPENSSSH 3.4p1–3 on AIX 4.3.3

>  
>  
>  
>  
>Alf,  
>  
>*I am assuming the you have RhostsAuthentication set to yes and*  
>*IgnoreRhosts set to no in the servers sshd\_config. If so do you have*  
>*reverse dns setup properly for that client? Also what is the setting of*  
>*the servers VerifyReverseMapping since it looks like you are failing on the*  
>*reverse dns lookup.*  
>  
>Neil  
>Alf Nicolaysen wrote:  
>  
>Neil,  
>  
>*thx for your answer so far. I tested it immediately and: It did not work!*  
>*Here`s the output for the server in debug modus:*  
>  
>*debug1: Server will not fork when running in debugging mode.*  
>*Connection from 9.164.18.128 port 982*  
>*debug1: Client protocol version 1.5; client software version OpenSSH\_3.4p1*  
>*debug1: match: OpenSSH\_3.4p1 pat OpenSSH\**  
>*debug1: Local version string SSH-1.99-OpenSSH\_3.4p1*  
>*debug2: Network child is on pid 27530*  
>*debug1: Sent 768 bit server key and 1024 bit host key.*  
>*debug1: Encryption type: 3des*  
>*debug2: monitor\_read: 28 used once, disabling now*  
>*debug2: monitor\_read: 30 used once, disabling nowdebug1: cipher\_init: set*  
>*keylen (16 -> 32)*  
>  
>*debug1: cipher\_init: set keylen (16 -> 32)*  
>*debug1: Received session key; encryption turned on.*  
>*debug1: Installing crc compensation attack detector.*  
>*debug2: monitor\_read: 6 used once, disabling now*  
>*debug1: Attempting authentication for nicolays.*  
>*Failed none for nicolays from 9.164.18.128 port 982*  
>*Could not reverse map address 9.164.18.128.*  
>*debug2: auth\_rhosts2: clientuser nicolays hostname 9.164.18.128 ipaddr*  
>*9.164.18.128*  
>*debug1: temporarily\_use\_uid: 201/1 (e=7)*  
>*debug1: restore\_uid*  
>*Failed rhosts for nicolays from 9.164.18.128 port 982 ruser nicolays*  
>*debug1: rcvd SSH\_CMSG\_AUTH\_TIS*  
>*Failed challenge-response for nicolays from 9.164.18.128 port 982*  
>  
>*As you can, the client uses an privileged Port and shows up protocol 1.5.*  
>*At the end of this output, two things are suspicious:*  
>  
>*1)Seems to have name-resolution problems with this IP-Adress 9.164.18.128*

SecurityFocus Secure Shell: Re: OPENSSSH 3.4p1-3 on AIX 4.3.3

>(the client of course), but DNS is ok  
>2)Why at the end the server tries to authenticate via the TIS-Auth??  
>  
>Further ist says "Failed rhosts for nicolays from 9.164.18.128 port 982"  
>What does it exactly mean? Couldn't the server READ the rhosts, in this  
>case .shosts? Or couldn't he simply not find it? Or wrong permissions ?  
>(Strictmode is set to default = no)  
>  
>Any more help is very much appreciated.  
>  
>Thx in advance  
>  
>  
>  
>  
>Alf Nicolaysen  
>  
>  
>  
>Neil Martin <[Neil@Car-Part.com](mailto:Neil@Car-Part.com)> on 13.02.2003 21:51:54  
>  
>To: Alf Nicolaysen/Germany/Contr/IBM@IBMDE  
>cc:  
>Subject: Re: OPENSSSH 3.4p1-3 on AIX 4.3.3  
>  
>  
>  
>Alf,  
>  
>I got that working under 3.5 on Solaris using .rhosts by doing something  
>like ssh -o "RhostsAuthentication yes" -o "UsePrivilegedPort yes" -o  
>"Procotol 1". It should work for .shosts  
>  
>It appears that the version 2 Protocol will not allow rhosts  
>authentication. In order to use the privileged port (low ports) you  
>will need to set the suid bit on ssh or run ssh from the root account.  
>This is very dangerous and insecure since someone would just need to  
>spoof one of your clients IP's and they are in. The recommended method  
>(under 2.0 of the protocol) would be to use ssh-agent to remember your  
>clients pass phrases. This is less vulnerable to spoofing.  
>  
>  
>Hope this helps.  
>  
>Neil  
>Alf Nicolaysen wrote:  
>  
>  
>  
>Hi all!  
>

SecurityFocus Secure Shell: Re: OPENSSSH 3.4p1-3 on AIX 4.3.3

>I try to substitute a normal rsh/rlogin environment to a ssh-environment  
>on some AIX 4.3.3 machines. For this environment I want to establish a  
>PasswordAuthentication (with all his security risks) and, if present, a  
>secure login without password using .shosts. Here starts the problem.  
>  
>  
>There  
>  
>  
>is no way, as far as I tested, to use a .shosts file. In any case this  
>  
>  
>file  
>  
>  
>will be ignored, regardless of modes, ownerships or user.  
>  
>There a two ways of logging into a machine: 1) A normal ssh to a machine  
>  
>  
>and  
>  
>  
>i have to give the password.  
>2) I first copy the id\_rsa.pub of the user into the authorized\_keys of the  
>second machine and then i can login into the machine without password.  
>  
>With RhostsAuthentication, I get the only worthful message into the debug  
>message:  
>  
>debug1: Rhosts Authentication disabled, originating port 33754 not  
>  
>  
>trusted.  
>  
>  
>How can the server machine trust a non-privileged port, that is choosen  
>randomly??  
>  
>What went wrong here?  
>  
>regards  
>  
>  
>  
>Alf Nicolaysen  
>  
>  
>  
>

>  
>  
>  
>  
>  
>  
>  
>  
>  
>  
>  
>  
>  
>  
>