

PuTTY failing "Server's host key did not match the signature supplied" suddenly

PuTTY failing "Server's host key did not match the signature supplied" suddenly

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2008-03/msg00019.html>

- *From:* Raymond <rpau88@xxxxxxxxx>
 - *Date:* Sun, 9 Mar 2008 18:03:57 -0700 (PDT)
-

Dear All,

PuTTY suddenly fails to connect to my server reporting "Server's host key did not match the signature supplied".

Configuration as follows:

PuTTY Version: Release 0.60

Server: CentOS release 5 (Final) with openssh-server-4.3p2-24.el5
openssh-4.3p2-24.el5

Tried connecting with ssh client and ssh reports:
"hash mismatch
key_verify failed for server_host_key"

or

"RSA_public_decrypt failed: error:0407006A:rsa
routines:RSA_padding_check_PKCS1_type_1:block type is not 01
key_verify failed for server_host_key"

Have anyone encountered this problem before?

Connection to other server is ok.

Regards,

Raymond Pau

.