Rumen Kasabov  
ID: 10128754  
Tutorial Section: T02  
Group partner: Michael Radke

The code is compiled the same way as the original version.

~~~

The vulnerability bug consists of the input char buffer not sanitizing values that are over 32 bytes long (the length of that buffer). Once the server is started, the input buffer, password buffer and the secret buffer are initialized in stack memory. In the original code, each buffer consists of 32 bytes (excluding the secret passphrase buffer).

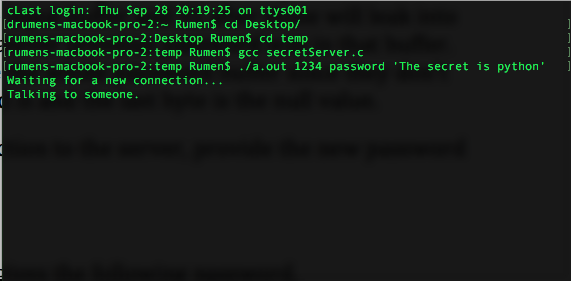
To exploit the bug, the attacker needs to connect to the server and provide an input that is 63 bytes long, where the first 32 characters (bytes) can be any random garbage value and the next 31 needs to be the password that they so choose. The first 32 characters will overwrite the input buffer and 31 after those will leak into the password buffer overwriting whatever previous password was in that buffer. Here the attacker needs to overwrite the whole password buffer since they don’t know how long the original password is and the last byte is the null character.

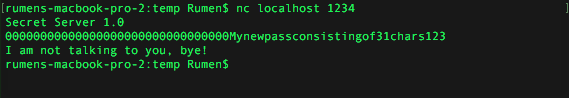
Then they can initialize a new connection to the server, provide the new password and uncover the secret pass phrase.

Sample exploit:

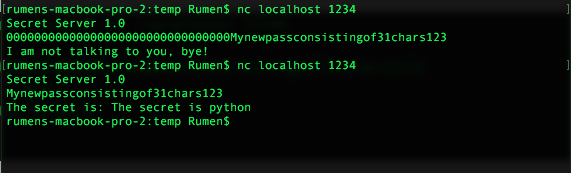
The user connects to the server and gives the following password,

$00000000000000000000000000000000Mynewpassconsistingof31chars123

Server connection with specified password and passphrase talking to attacker



Attacker exploits vulnerability by giving the above password. The first 32 bytes fill up the buffer and the next 31 overflow into the password buffer, overwriting the original password.



The attacker now enters the new password in and obtains the secret passphrase.