Pidgin Client Password Disclosure Vulnerability

Credit: Aditya K Sood , Founder SecNiche Security

Release Date: 11 September 2008

About Pidgin: Pidgin 2.5.1

Pidgin is a graphical modular messaging client based on libpurple which is capable of connecting to AIM, MSN, Yahoo!, XMPP, ICQ, IRC, SILC, SIP/SIMPLE, Novell GroupWise, Lotus Sametime, Bonjour, Zephyr, MySpaceIM, Gadu-Gadu, and QQ all at once. It is written using GTK+.

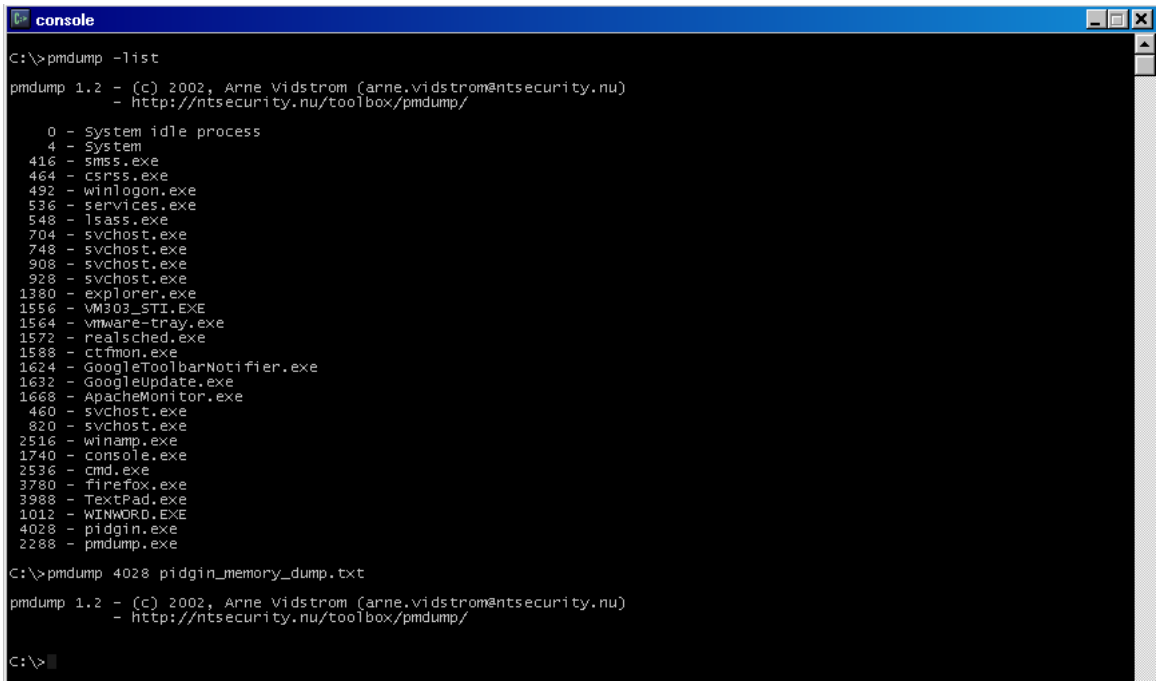
Explanation:

The pidgin client inherits client side password disclosure vulnerability. The credentials used to connect to the required service i.e. username and password is not encrypted properly. The credentials can be extracted in clear text by dumping process memory of the live pidgin process when a connection is set. The vulnerability allows anyone with access to the client system to obtain the username and password. Additionally, this vulnerability could also be exploited by fooling the user to execute malicious code which would dump the memory of the process "pidgin.exe".

Description:

A test account is created with username “pidgin_test” and password “memorypass”. Live connection is set to the yahoo service. The process is dumped and analyzed to prove the concept.

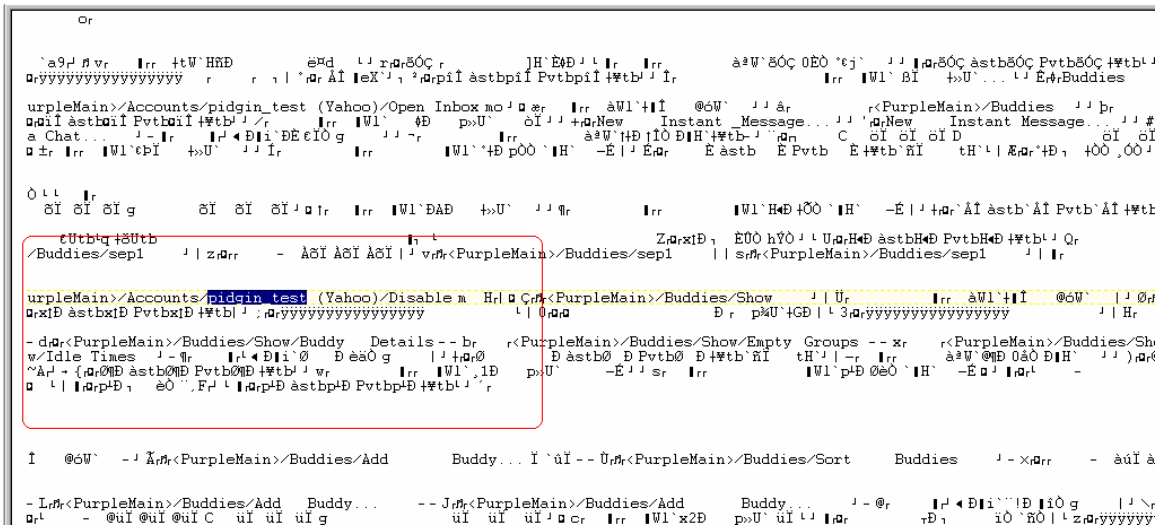
Step 1: Dumping memory with pmdump utility



The pidgin memory dump is extracted to a txt file for analysis.

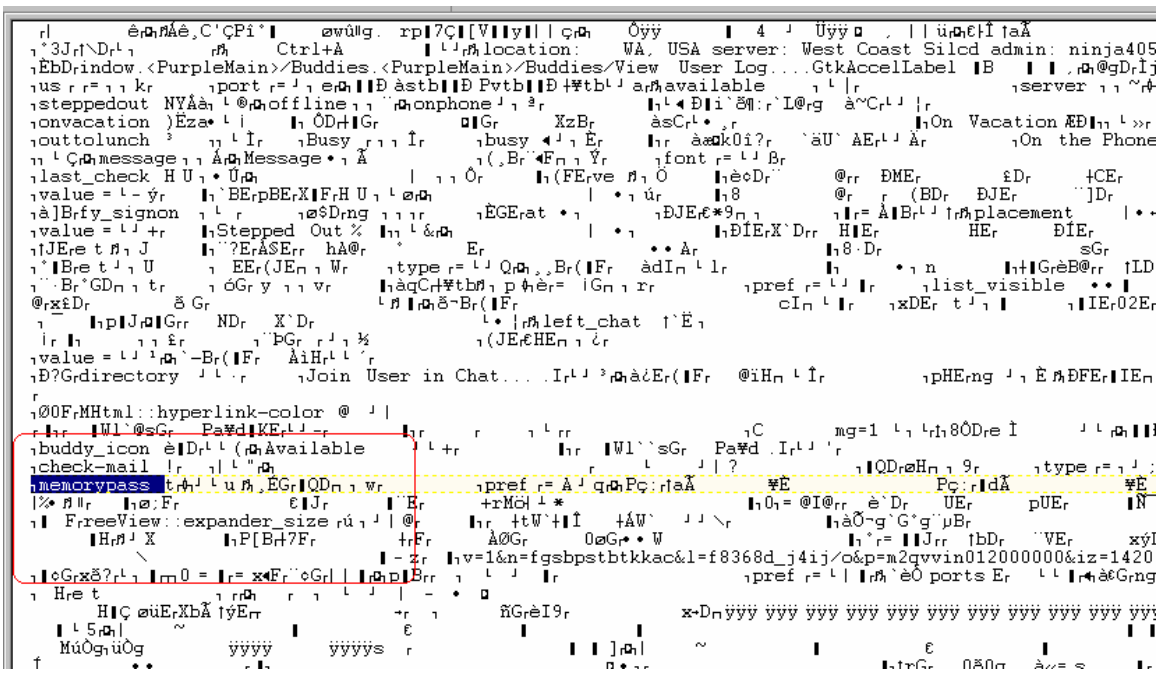
Step 2: Analyzing Dumps

The analysis shows the **"pidgin_test"** user account has 25 clear text entries in the memory dump.



The username can be seen in clear text.

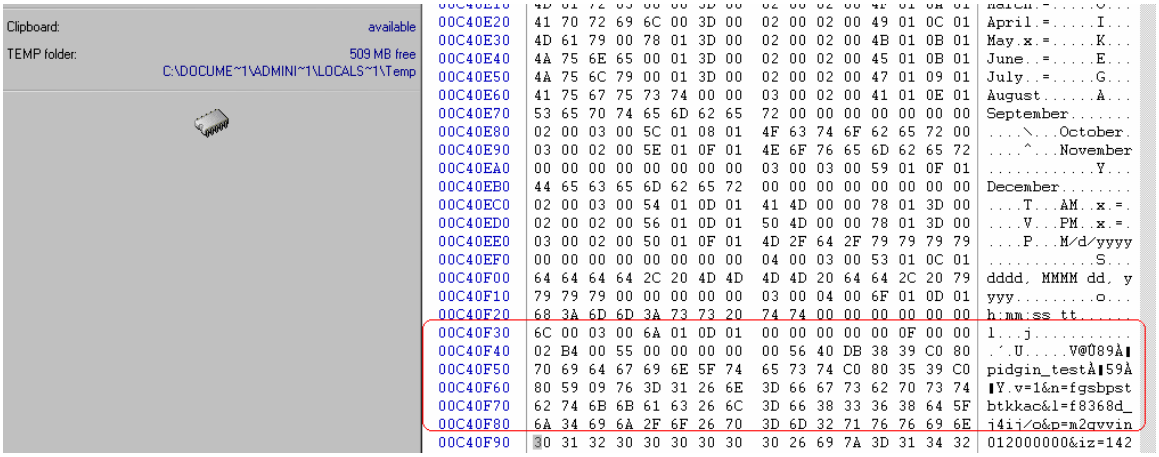
The password **"memorypass"** is appeared 2 times.



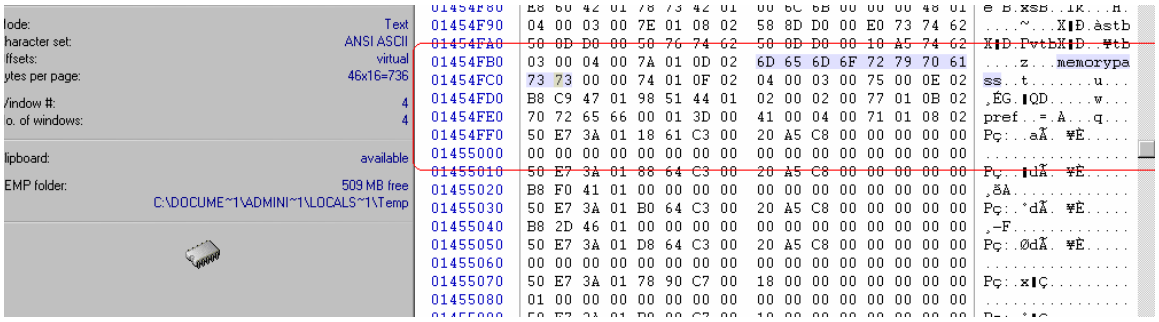
The password can be seen in clear text.

Step 3: Cross Check with WinHex.

3.1 User Check



3.2 Password Check



The POC is done.

Disclaimer:

The information in the advisory is believed to be accurate at the time of publishing based on currently available information. Use of the information constitutes acceptance for use in an AS IS condition. There is no representation or warranties, either express or implied by or with respect to anything in this document, and shall not be liable for a ny implied warranties of merchantability or fitness for a particular purpose or for any indirect special or consequential damages.

Contact:

Adi_ks [at] secniche.org