Advisory :
PidginIM Client Password Disclosure Vulnerability.

Version Affected:

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+.

Release Date:
11 September 2008
.

Description:

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".

Proof of Concept:
Download: http://www.evilfingers.com/advisory/pidgin_password_disc_vuln.pdf

Credit:
Aditya K Sood
Team Lead, www.EvilFingers.com

http://www.secniche.org

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.