AIX PLATFORM SPECIFIC SECURITY PATCHES

This appendix deals with vendor-provided patches that **MUST** be installed to properly secure an IBM AIX Unix system. When IBM is informed of or discovers a vulnerability, they will issue what is known as an APAR (Authorized Program Analysis Report) concerning the defect in the software product. At some point, IBM will issue a PTF (Program Temporary Fix), that will correct the defect.

APAR's and PTF's can be obtained directly from IBM by calling 1-800 237-5511, by downloading and utilizing the FixDist application, or in some cases, by contacting the AIX help desk at 314 235-2985 where the patch can be mounted to your system.

The FixDist application is freely available from IBM at http://service.software.ibm.com via a WEB browser or via anonymous ftp at service.software.ibm.com (198.17.57.66) in the aix/tools/fixdist directory. This application allows the sysadmin to obtain the appropriate patch either by APAR or PTF id when it becomes available. Once the fix is obtained, it can be installed using the SMIT utility.

Following is a matrix that identifies the vulnerable area, the operating system level, and the APAR and PTF id. To determine if a fix has been installed, issue the command:

lslpp -al <PTF #> for versions below 4.0

instfix -ik <APAR #> for versions 4.0 and above

In addition, insure that the fix has been committed and not just copied to the system.

VULNERABILITY	OPERATING SYSTEM	APAR #	PTF #
REXD DAEMON	3.2.4 & BELOW	IX21353	U442638
YPBIND	3.2.5	IX43595	U442638
PASSWD COMMAND	3.2.x	IX23505	U434998
CRONTAB COMMAND	3.2.x	IX26997	U435236
CRON DAEMON	3.2.x	IX46848	U435351
CRON	3.2.x	IX47706	U441405
PERFORMANCE TOOLS	3.2.5 & 3.2.4 Systems with PTFs U420020 & U422510 installed	IX42332	U427873
BATCH QUEUE	3.2.x & BELOW	IX44381	U432030
LOGIN	3.2.x	IX44254	U431620 &U431909
SYSLOG LOGGING	3.2.x	IX42340	U428937
CRASH COMMAND	3.2.x	IX43399 IX44274	U430280
RACE CONDITION	3.2.x	IX43484	U431052
REMOTE QUEUE	3.2.x	IX45366	U432843
UMASK	3.2.x	IX44735	U435125
/USR/LIB/RAS	3.2.x	IX45372	U435238
RSH/REXEC	3.2.x	IX45701	U434997,U434998, U535113,U435114, U435128
PERFORMANCE TOOLS	3.2.x	IX46153	U435122
AIXTERM LOGGING	3.2.x	IX46360	U435140
PORTMAPPER	3.2.x	IX32328	U435180,U435128, U428287
XTERM -X11R4	3.2.x	IX40279	U428187,U428066
XTERM-X11R5	3.2.x		U493250
RPC.YPUPDATED	3.2.x	IX55360	U440666
RPC.YPUPDATED	4.1.x	IX55363	U441187
RMAIL	3.2.x	IX57680	
PCNFSD	3.2.x	IX57623 & IX56965	U442633,U442638
PCNFSD	4.1.x	IX57616 & IX56730	
RPC.STATD	3.2.x	IX56056	U441411
RPC.STATD	4.1.x	IX55931	
SYSLOG DAEMON	3.2.x	IX53358	U440272
SYSLOG DAEMON	4.1.x	IX53718	
SENDMAIL	3.2.x	IX61303 IX61307 IX64460	☞
SENDMAIL	4.1.x	IX61162	☞

VULNERABILITY	OPERATING SYSTEM	APAR #	PTF #
		IX61306 IX64459	
SENDMAIL	4.2	IX61304 IX61305 IX63068 IX64443	☞
XDM	3.2.5	IX54679	NUMEROUS
XDM	4.1.x	IX54680	
RDIST	3.2.x	IX59741	
RDIST	4.1.x	IX59742	
RDIST	4.2	IX59743	
LQUERYPV	4.1	IX64203	
LQUERYPV	4.2	IX64204	
IP SPOOF	3.2.x	IX59644	
IP SPOOF	4.1.x	IX58507	
IP SPOOF	4.2	IX58905	
GETHOSTBYNAME	3.2.x	IX60927	U443452 U444191 U444206 U444213 U444233 U444244
GETHOSTBYNAME	4.1.x	IX61019	
GETHOSTBYNAME	4.2.x	IX62144	
/USR/SBIN/ROUTE	4.1.x	IX54674	
SYN FLOOD	4.1.x	IX62476	
SYN FLOOD	4.2.x	IX62428	
RLOGIN	3.2.x	IX57724	
RLOGIN	4.1.x	IX57972	
TALKD	3.2.x	IX65474	
TALKD	4.1.x	IX65472	
TALKD	4.2.x	IX65473	
PING ATTACK	3.2.x	IX59644	U444227 U444232
PING ATTACK	4.1.x	IX59453	
PING ATTACK	4.2.x	IX61858	

☞ If you are running Blair Porter's sendmail version 8.8.x, available from bedrock under mail/sendmail/AIX, it is not necessary to install this PTF.

IBM X-STATION 140, 150, 160

IBM's X-Stations have their own unique security vulnerabilities. Following are the steps necessary to properly secure these X-stations.

X-TERMINALS 140 AND 150

A vulnerability exists in IBM's 140 and 150 X terminals that allow anyone on the TCP/IP network to access the X terminals with limited privileged access.

Once the terminals are booted from a server, the X terminals are given a unique IP address, whereby anyone on the TCP/IP network can "rlogin" or "rsh" to the addresses without login and password authentication. However, it appears that this kind of access allows only limited privileged. For example, if a "?" is issued at the prompt, a list of commands are displayed that are accessible by the user (e.g., kill, ps, cat, etc.).

```
xs140:?

  Help        - print this list
  ?           - print this list
  time        - measure command execution time
  sleep       - sleep a specified number of seconds
  add_cmd     - add a new builtin command to the system
  rem_cmd     - remove a builtin command from the system
  start_cmd   - start a command with specified priority or stacksize
  shell       - usage: shell [-f file]
  ps          - print process status of local clients
  text        - show info on dloaded obj files. usage: text [-r][-s]
  dload       - usage: dload [-k stk][-b][-n][-r][-s][-l lib][-d] cmd
  setenv      - usage: setenv VAR=value
  printenv    - usage: printenv [VAR]
  rlogin      - usage: rlogin hostname [ -l username ]
  telnet      - Usage: telnet hostname
  rsh         - usage: rsh host [cmd]
  echo        - echo arguments
  cat         - usage: cat file1 [ file2 ... ]
  print       - usage: print device [ port ]
  ifstat      - usage: ifstat [if_name]
  tty         - Display terminal name if a tty. usage: tty
  stty        - Display/set terminal modes. usage: stty [option]
  netstat     - print network statistics
  device_session  - device_session dev [ port ]
  devices     - Display list of devices
  memavl      - usage: memavl [-u]
  ls          - usage: ls [ directory ]
  cd          - usage: cd [ dirname ]
  pwd         - print current working directory
  stack       - stack [-p pid]
```

pipe - usage: pipe cmd1 cmd2
page - usage: page [file]
kill - usage: kill [-signal] pid_list
source - usage: source file_list

IBM has issued a patch(1.7) to disable this vulnerability. Software release 1.8 will password protect this feature.

****

X-TERMINAL 160

XHOST Vulnerabilities with IBM Xstation 160, has been a long term problem. This vulnerability allowed anyone that got access to the network the ability to capture all key strokes, a picture of the screen, or actually take control of the vulnerable terminal.

To configure the IBM Xstation 160 securely:

Upgrade the Xstation 160 to Version 1.6 or better. The upgrade can be obtained from IBM on tape or from their home page.

To begin the configuration enter the configuration menu by pressing CTL ALT Backspace.

Go into the MAIN menu.
Click on Advance.
Click on Host Access Control.
Click on Enable.
Click on Table.
Enter IP of host to trust.
Click on verify.
Click on TABLE.

To add additional Hosts enter the IP.
Click on verify.
Click on add after or add before.

The /etc/X0.host file on the system that the Xstation boots from should include the systems you want to trust.