HEWLETT-PACKARD PLATFORM SPECIFIC SECURITY PATCHES

This appendix deals with vendor-provided patches that **MUST** be installed to properly secure a HP-UX Unix system. When HP is informed of or discovers a vulnerability, they will issue what is known as a HPSB (Hewlett-Packard Security Bulletin) concerning the defect in the software product. The bulletin will contain a patch identification number that can be retrieved to correct the defect.

THE RECOMMENDED METHODOLOGY FOR OBTAINING HP's patches is to contact the HP help desk at 314 235-2980. The HP help desk has a patch server available that does not require a browser or Internet access. Other methodologies for obtaining patches follow:

HP SupportLine Registration Instructions

HP SupportLine phone number: 415-691-3888.

There are three categories for obtaining the security patches:

1. Eligible HP SupportLine customers (who have a software support contract or have recently purchased an HP 9000) who access via a terminal or modem.
2. Eligible HP SupportLine customers who would access via Internet.
3. Customers not currently accessing HP SupportLine.

Category 1:

Step 1: Dial 415-691-3680.

Step 2: When your communications program indicates that you are connected, press "return". The system prompt, ":" or "login:", should appear.

Step 3: If your system prompt is ":", log on to the HP SupportLine account by typing "HELLO USER.HPSL", followed by "return".

If your system prompt is "login:", log on by typing "login: hpsl", followed by "return".

Step 4: When prompted, type your system handle and password, each followed by "return". Both your system handle and password are provided in the cover letter you received with your "Getting Started Kit".

Step 5: Press "return" until the HP SupportLine Top Menu screen is displayed. If your terminal does not support block mode, you should enable HPSL's line editor by typing "SET

EDITOR LINE" at the command prompt and entering "return".

Category 2:

Step 1: HP 9000, HP Apollo, and HP 64000 system users who have been authorized by the National Science Foundation (NSF) to use Internet may access HP SupportLine over the Internet. Connect to HP SupportLine using the address provided in your "Getting Started Kit".

An example U.S. login is

```
telnet 192.6.148.19
or
telnet support.mayfield.hp.com
```

Step 2: Once you access HP SupportLine, type "hpsl" at the "login:" prompt.

Step 3: When prompted, enter your system handle and password, each followed by "return". Both your system handle and password are provided in the cover letter you received with your "Getting Started Kit".

Step 4: Press "return" until the HP SupportLine Top Menu is displayed.

Step 5: At the Top Menu, choose "3 Patch support information" by typing "3" at the "Select an item or enter a command (? for help) :" prompt. This will put you in the Patch Support Information Menu.

Step 6: At the Patch Support Information Menu, choose "3 Retrieve patch file transfer login" to get your patch file transfer login by typing "3" at the "Select an item or enter a command (? for help) :" prompt. This will put you at a screen to choose the method for patch file transfers. The choices are ftp, kermit, and uucp.\
To choose ftp, type "1" at the "Enter selection :" prompt. The next screen will display your patch file transfer method and your patch file transfer login. You will use the *SAME* patch file login when you ftp patch file(s).

Step 7: When you exit the HP SupportLine, by typing "E" at the "Select an item or enter a command (? for help) :" prompt, the connection is closed.

Step 8: FTP to

```
192.6.148.19
or
support.mayfield.hp.com
```

Step 9: At the "Name (support.mayfield.hp.com:username):" prompt, type your patch file transfer login.

Step 10: At the "Password:" prompt, type your password assigned to you by Hewlett-Packard when you registered.

Step 11: At the "ftp>" prompt, set the transfer mode to binary by typing "bin". You should get a message "Type set to I".

Step 12: At the "ftp>" prompt, cd to "hp-ux_patches". Then cd to the directory named for your type of architecture (s300_400, s700, or s800). Then cd to "8.X".

Step 13: At the "ftp>" prompt, type "get PHNE_xxxx" (where xxxx is 1359, 1360, or 1361 - depending on the architecture of your host(s)).

Category 3:

Step 1: Dial 415-691-3680.

Step 2: Type "hpslreg" at the "login:" prompt to begin the registration process.

Step 3: Follow the instructional prompts.

Step 4: Once you have received your HP SupportLine system handle and password, follow the directions in category 1) or 2), depending on your preferred access method.

HP Patch Retrieval Instructions

HP SupportLine phone number: 415-691-3888.

Please retain (PRINT) the following login instructions for your records.
Your System Handle and Password needed to access HP SupportLine are:

SYSTEM HANDLE :
PASSWORD :

HP SupportLine can be accessed in three ways:

1. CompuServe members may type GO HPSL from the top menu.
2. Internet users may connect using the I. P. address 192.6.148.19.
3. Or you can direct dial HP SupportLine by redialing (xxx) xxx-xxxx.

After using any of the above access methods, follow these instructions:

1. To login to HP Supportline, respond to the prompt with `hpsl'.
2. When prompted, respond with your System Handle and Password.

Following is a matrix that identifies the vulnerable area, the operating system level, and the

Patch identifier. To determine if a fix has been installed, issue the command:

ls -al /system/PH<patch identifier> for versions below 10.0

swlist -l product | grep PH<patch identifier> for versions 10.0 and above

VULNERABILITY	OPERATING SYSTEM/SERIES	PATCH IDENTIFIER
X-TERM	HP-UX 8.x 300	PHSS_4216
X-TERM	HP-UX 9.x 300	PHSS_5031
X-TERM	HP-UX 9.x 700/800	PHSS_5902
SENDMAIL	HP-UX 8.x 300	PHNE_5383 ☞
SENDMAIL	HP-UX 8.x 700/800	PHNE_5401 ☞
SENDMAIL	HP-UX 9.x 300	PHNE_5384 ☞
SENDMAIL	HP-UX 9.01,3,5,7 700	PHNE_9621 & PHNE_10033 ☞
SENDMAIL	HP-UX 9.09 700	PHNE5387 & PHNE 5388 ☞
SENDMAIL	HP-UX 9.00,4 800	PHNE_9621 & PHNE_10033 ☞
SENDMAIL	HP-UX 9.08 800	PHNE_5389 ☞
SUBNETCONFIG	HP-UX 9.x 300	PHNE_3563
SUBNETCONFIG	HP-UX 9.x 700/800	PHNE_3564
HPTERM	HP-UX 8.x 300	PHSS_5549
HPTERM	HP-UX 8.07 700	PHSS_4525
HPTERM	HP-UX 8.x 800	PHSS_4526
HPTERM	HP-UX 9.00 & 9.03 300	PHSS_4527 & PHSS_5438
HPTERM	HP-UX 9.10 300	PHSS_5438
HPTERM	HP-UX 9.x 700/800	PHSS_6155 & PHSS_7751
DCE/9000	HP-UX 9.x 700/800	PHSS_3820
DCE KEY GENERATE	HP-UX 9.03,5,7 700	PHSS_8340 & PHSS_6921
DCE KEY GENERATE	HP-UX 9.04 800	PHSS_8340 & PHSS_6921
DCE KEY GENERATE	HP-UX 10.01 700/800	PHSS_8342
DCE KEY GENERATE	HP-UX 10.10 700/800	PHSS_8344
HP VUE 3.0	HP-UX 9.x 300	PHSS_5438
HP VUE 3.0	HP-UX 9.x 700/800	PHSS_7751
HP VUE 3.0	HP-UX 10.01 700/800	PHSS_7752
HP VUE 3.0	HP-UX 10.10 700/800	PHSS_7753
OSF/AES STANDARD	HP-UX 9.01 700	PHCO_5588 & PHKL_9148
OSF/AES STANDARD	HP-UX 9.03,5,7 700	PHCO_5588 & PHKL_9868
VHE_U_MNT	HP-UX 8.00 300	PHNE_4363
VHE_U_MNT	HP-UX 9.00,03 300	PHNE_4363
VHE_U_MNT	HP-UX 8.x 700/800	PHNE_4434
X-AUTHORITY	HP-UX 9.01,3,5 700	PHSS_5568
CORE-DIAG FILESET	HP-UX 8.x 700	PHSS_4574
CORE-DIAG FILESET	HP-UX 8.00,6 800	PHSS_4578
CORE-DIAG FILESET	HP-UX 8.02 800	PHSS_4577
CORE-DIAG FILESET	HP-UX 9.01 700	PHSS_4475
CORE-DIAG FILESET	HP-UX 9.03,5,7 700	PHSS_8572

VULNERABILITY	OPERATING SYSTEM/SERIES	PATCH IDENTIFIER
CORE-DIAG FILESET	HP-UX 9.00 800	PHSS_4660 & PHSS_4989
CORE_DIAG FILESET	HP-UX 9.04 800	PHSS_6683
XWCREATE/GWIND	HP-UX 8.x 300	PHSS_4836
XWCREATE/GWIND	HP-UX 8.07 700	PHSS_4834
XWCREATE/GWIND	HP-UX 8.x 800	PHSS_4835
XWCREATE/GWIND	HP-UX 9.00,3 300	PHSS_4833
XWCREATE/GWIND	HP-UX 9.x 700/800	PHSS_5140
SUPPORT WATCH	HP-UX 8.x 800	PHSS_4874
SUPPORT WATCH	HP-UX 9.00 800	PHSS_4874
REMOTE WATCH	HP-UX 8.x 300	PHSS_5168
REMOTE WATCH	HP-UX 9.x 300	PHSS_5120
REMOTE WATCH	HP-UX 8.x 700	PHSS_5180
REMOTE WATCH	HP-UX 8.x 800	PHSS_5185
REMOTE WATCH	HP-UX 9.x 700	PHSS_5107
REMOTE WATCH	HP-UX 9.x 800	PHSS_5136
CODING SEQUENCES	HP-UX 9.01 700	PHKL_5048
CODING SEQUENCES	HP-UX 9.03,5,7 700	PHKL_9868
CODING SEQUENCES	HP-UX 9.09 700	PHKL_5190 & PHKL_6591
CODING SEQUENCES	HP-UX 9.00 800	PHKL_5050
CODING SEQUENCES	HP-UX 9.04 800	PHKL_9230
CODING SEQUENCES	HP-UX 9.08 800	PHKL_5192
AT & CRON	HP-UX 8.00 300	PHCO_5443
AT & CRON	HP-UX 8.x 700	PHCO_5203
AT & CRON	HP-UX 8.x 800	PHCO_5204
AT & CRON	HP-UX 9.00,3 300	PHCO_5206
AT & CRON	HP-UX 9.01,3,5,7 700	PHCO_6861
AT & CRON	HP-UX 9.00,4 800	PHCO_7030
FTP	HP-UX 9.x 300	PHNE_6146 ☞☞
FTP	HP-UX 9.01,3,5,7 700	PHNE_6013 ☞☞
FTP	HP-UX 9.09 700	PHNE_6169 & 6170 ☞☞
FTP	HP-UX 9.00,4 800	PHNE_6013 ☞☞
FTP	HP-UX 9.08 800	PHNE_6171 ☞☞
FTP	HP-UX 10.00,01,10 700	PHNE_9181 ☞☞
FTP	HP-UX 10.09 700	PHNE_5965 ☞☞
FTP	HP-UX 10.x 800	PHNE_9181 ☞☞
SYSLOG ROUTINE	HP-UX 9.x 300	PHCO_6224
SYSLOG ROUTINE	HP-UX 9.01,3,5,7 700	PHCO_9776
SYSLOG ROUTINE	HP-UX 9.09 700	PHCO_6160 & PHCO_6161
SYSLOG ROUTINE	HP-UX 9.00,4 800	PHCO_9777
SYSLOG ROUTINE	HP-UX 9.08 800	PHCO_6162
SYSLOG ROUTINE	HP-UX 10.00,01 700/800	PHCO_9419
SYSLOG ROUTINE	HP-UX 10.09 700	PHCO_6157
GLANCEPLUS	HP-UX 9.x 700	PHSS_8231

PROPRIETARY
Not for use or disclosure outside of Southwestern Bell
except under written agreement.

VULNERABILITY	OPERATING SYSTEM/SERIES	PATCH IDENTIFIER
GLANCEPLUS	HP-UX 9.x 800	PHSS_8232
GLANCEPLUS	HP-UX 10.01 700/800	PHSS_8233
GLANCEPLUS B.10.13	HP-UX 10.10 700/800	PHSS_9116
GLANCEPLUS B.10.10 B.10.11 or B.10.12	HP-UX 10.10 700/800	PHSS_9524
GLANCEPLUS	HP-UX 10.20 700/800	PHSS_9117
EXPRESERVE	HP-UX 9.x 700/800	PHCO_6363
EXPRESERVE	HP-UX 9.x 300	PHCO_7833
EXPRESERVE	HP-UX10.01 700/800	PHCO_8652
EXPRESERVE	HP-UX 10.10 700/800	PHCO_9489
EXPRESERVE	HP-UX 10.20 700/800	PHCO_8654
RPC.PCNFSD RPC.STATD PORTMAPPER NFS/NIS	HP-UX 9.x 300	PHNE_7371 & PHNE_7372
RPC.PCNFSD RPC.STATD PORTMAPPER NFS/NIS	HP-UX 9.00, 04 800	PHNE_9463
RPC.PCNFSD RPC.STATD PORTMAPPER NFS/NIS	HP-UX 9.09 700	PHNE_8016 & PHNE_8017
RPC.PCNFSD RPC.STATD PORTMAPPER NFS/NIS	HP-UX 9.01,3,5,7 700	PHNE_9463
RPC.PCNFSC RPC.STATD PORTMAPPER NFS/NIS	HP-UX 9.08 800	PHNE_8015
RPC.PCNFSD RPC.STATD PORTMAPPER NFS/NIS	HP-UX 10.00,01,10 700/800	PHNE_9464
RPC.PCNFSD RPC.STATD PORTMAPPER NFS/NIS	HP-UX 10.09 700	PHNE_8018 & PHNE_8019
RPC.PCNFSD RPC.STATD PORTMAPPER NFS/NIS	HP-UX 10.09 800	PHNE_8019
RPC.PCNFSD	HP-UX 10.16 700/800	PHNE_8020

VULNERABILITY	OPERATING SYSTEM/SERIES	PATCH IDENTIFIER
RPC.STATD PORTMAPPER NFS/NIS		
ELM	HP-UX 9.x 300	PHCO_7204
ELM	HP-UX 9.x 700/800	PHNE_9164
ELM	HP-UX 10.x 700/800	PHNE_9859
RDIST	HP-UX 10.00, 01 700/800	PHCO_9419 & PHNE_9217
RDIST	HP-UX 10.10 700/800	PHNE_9218
RDIST	HP-UX 10.20 700/800	PHNE_9219
DIRECT AUDIO	HP-UX 10.10 700	PHKL_9579
DIRECT AUDIO	HP-UX 10.20 700	PHKL_9580
NEWGRP COMMAND	HP-UX 9.X	PHCO_9603
NEWGRP COMMAND	HP-UX 10.00,01	PHCO_9604
NEWGRP COMMAND	HP-UX 10.10,20	PHCO_9605
AUTHENTICATION	HP-UX 10.10 700/800	PHSS_8665 & PHSS_9690
AUTHENTICATION	HP-UX 10.20 700/800	PHSS_8667 & PHSS_9627
PASSWD	HP-UX 9.0,04 800	PHCO_9742
PASSWD	HP-UX 9.01,03,05,07 700	PHCO_9743
PASSWD	HP-UX 10.00,01 700/800	PHCO_7635 & PHCO_9640
PASSWD	HP-UX 10.10 700/800	PHCO_7394 & PHCO_9640
PASSWD	HP-UX 10.20 700/800	PHCO_9641
CHSH	HP-UX 9.X 700/800	PHCO_9600
CHSH	HP-UX 10.00,01,10 700/800	PHCO_9601
CHSH	HP-UX 10.20 700/800	PHCO_9602
CHFN	HP-UX 9.X 700/800	PHCO_9595
CHFN	HP-UX 10.00,01,10 700/800	PHCO_9596
CHFN	HP-UX 10.20 700/800	PHCO_9597
LARGE UID'S & GID'S	HP-UX 10.20	PHSS_9343 & PHNE_9377 & PHNE_9504
RLOGIN	HP-UX 9.X 700/800	PHNE_8805
RLOGIN	HP-UX 10.0X, 10.10 700/800	PHNE_8806
RLOGIN	HP-UX10.20 700/800	PHNE_8807
MPOWER	HP-UX 10.0,1X 700/800	PHNE_9773
MPOWER	HP-UX 10.20 700/800	PHNE_9669
PPL	HP-UX 9.X 700/800	PHNE_9378
PPL	HP-UX 10.00, 10.01 700/800	PHNE_9375
PPL	HP-UX 10.10 700/800	PHNE_9376
PPL	HP-UX 10.20 700/800	PHN3_9771
PING ATTACK	HP-UX 9.01 700	PHNE_7704 & PHNE_9027
PING ATTACK	HP-UX 9.03,05,07 700	PHNE_9100
PING ATTACK	HP-UX 10.0 700	PHNE_9030
PING ATTACK	HP-UX 10.01 700	PHNE_9102
PING ATTACK	HP-UX 10.10 700	PHNE_9104

VULNERABILITY	OPERATING SYSTEM/SERIES	PATCH IDENTIFIER
PING ATTACK	HP-UX 10.20 700	PHNE_9098
PING ATTACK	HP-UX 9.00 800	PHNE_7197 & PHNE_8672
PING ATTACK	HP-UX 9.04 800	PHNE_9101
PING ATTACK	HP-UX 10.00 800	PHNE_9031
PING ATTACK	HP-UX 10.01 800	PHNE_9103
PING ATTACK	HP-UX 10.10 800	PHNE_9105
PING ATTACK	HP-UX 10.20 800	PHNE_9099

☞ If you have installed Blair Porter's version 8.8.x of sendmail available from bedrock under /mail/sendmail/HP-UX, it is not necessary to install this patch.

☞☞ If you have installed the SecurID or TACACS+ versions of the ftp daemon, it is not necessary to install this patch.

There are several situations in the HP environment for which no patches have been released, but which require a fix by the SysAdmin. They are:

Multimedia Sharedprint Vulnerability
The HP-UX 9.x/series 700 fileset SHAREDPR-PCL contains files with permissions that allow a user to gain higher system privileges. To fix the problem do the following:

```
chmod 544 /usr/imaging/pcl/util/update_pcl_fonts
chmod 544 /usr/imaging/pcl/util/ssmak
chmod 544 /usr/imaging/pcl/util/ixmak
```

Vuelogin
Even if you have root login limited to the system console with the /etc/securetty file setup, someone with a X-terminal can still login directly as root. To fix this situation do:

Add the following lines to the end of the /usr/vue/config/Xstartup

```
if [ $USER = root ] ; then
   exit 1
fi
```

NETTUNE Vulnerability

The HP-UX 10.0 and 10.01 contain a vulnerability in the "nettune" utility program. In order to correct this vulnerability, the following commands **MUST** be issued:

```
chmod 555 /usr/contrib/bin/nettune
```

```
chown bin /usr/contrib/bin/nettune
```

SAM REMOTE ADMINISTRATION Vulnerability

The HP-UX 9.x and 10.x operating systems possibly contain a vulnerability with SAM remote administration that will allow an intruder root access to the system with a HP provided and widely-known default password. The general fix for this is **DO NOT** use this type of administration. To determine if the system contains this vulnerability, search the /etc/passwd file for the existence of a userid "sam_exec:*:0:1". If this userid exists, the system is at risk. There may also be a .rhost file under the sam_exec home directory which will allow some other system root access to this system. If the system is shadowed, look in the /.secure/etc/passwd file for the existence of "sam_exec:SA27aM8/b0isE:13:1" which is the default password that HP delivers. If any of these conditions exist:

Remove the .rhost file from the sam_exec home directory
Remove the sam_exec entry in the /.secure/etc/passwd file
Insure that there is an asterisk(*) in the passwd field in the /etc/passwd file

REMOTE WATCH Vulnerability

There are several vulnerabilities in HP's Remote Watch utility on the 10.X releases of Hp-UX which allow users to gain unauthorized root access. HP is not releasing any patches since SAM has replaced the functionality of Remote Watch. Consequently, the Remote Watch product must be removed from the system. To accomplish this execute:

```
/usr/remwatch/bin/removeall
```

Then remove the following entry from the /etc/inetd.conf file

```
rwdaemon stream tcp nowait root /usr/remwatch/bin/rwdaemon rwdaemon
```

Then refresh the inetd by issuing the command

```
inetd -c
```