SANTA CRUZ OPERATIONS (SCO) PLATFORM SPECIFIC SECURITY PATCHES

This appendix deals with vendor-provided patches that **MUST** be installed to properly secure a SCO Unix system. When Santa Cruz Operations is informed of or discovers a vulnerability, they will issue a (S)ystem (S)ecurity (E)nhancement, SSE to address the problem. These are preliminary patches which SCO believes addresses the immediate problem but may not be fully tested. Fully tested and integrated patches are available soon after in the form of a (S)upport (L)evel (S)upplement, SSL. The SSE and SLS will contain a patch identification number that can be retrieved to correct the defect. SSE's and SLS' can be directly obtained from a SCO ftp site "ftp.sco.Com" in the /SSE or /SLS directorys. Patch retrieval and installation instructions follow:

RETRIEVING AND INSTALLING A SSE

The System Security Enhancement directory (SSE) is here to provide timely fixes to problems with system security. Binaries acquired from this directory are to be considered preliminary fixes only and have not been fully tested or integrated. As such these patches are not officially supported. They are provided as a timely response to security concerns that have been brought to the attention of The Santa Cruz Operation.

When final approved patches are available usually by a Support Level Supplement the README files below will be modified to indicate the existence of the finalized version of the supplement. SCO reserves the right to change the contents of these supplements at any time.

The format of the Supplements found here are as follows:

ssexxx.tar.Z	- a compressed tar file
ssexxx.ltr.Z	- cover letter

release information and installation instructions

where xxx indicates the number of the supplement.

After downloading an SSE uncompress both the tar file and the coverletter. For example if you were trying to install SSE001 after downloading sse001.tar.Z and ssexxx.ltr.Z you would uncompress both files:

```
# uncompress ssexxx.tar.Z
# uncompress ssexxx.ltr.Z
```

After uncompressing both files you should then follow the instructions provided in the sse001.ltr file for installation instructions.

CONNECTION INFORMATION

For anonymous ftp connection:

Directory Name: /SSE

ftp to ftp.sco.com
Login name: ftp
Password: your email address

ftp to ftp.uu.net (NOTE: areas are located in the ./sco-archive directory)
Login name: ftp
Password: your email address

For anonymous UUCP connection:

Directory Name: /usr/spool/uucppublic/SSE

For USA, Canada, Pacific Rim, Asia and Latin America customers:

Machine name: sosco
Login name: uusls (fourth character is the letter l)
No password

List of modems available for UUCP transfer from sosco:

V32, V32bis	+408 425-3502
Telebit Trailblazer	+408 429-1786

For SCO Online Support (SOS) BBS download:

These supplements can be downloaded interactively via XMODEM, YMODEM ZMODEM or Kermit. Follow the menu selections under Toolchest from the main SOS menu.

List of modems available for interactive transfer from SOS:

V32, V32bis	+408 426-9495
Telebit Trailblazer	+408 426-9525

Note: telnet access to SOS is available by telneting to sos.sco.com

For customers with access to CompuServe:

Type GO SCOFORUM

For ftp via World Wide Web:

URL to open: ftp://www.sco.com

RETRIEVING AND INSTALLING A SLS

Directory Name: /SLS

ftp to ftp.sco.com
Login name: ftp
Password: your email address

ftp to ftp.uu.net (NOTE: areas are located in the ./sco-archive directory)
Login name: ftp
Password: your email address

For anonymous UUCP connection:

Directory name: /usr/spool/uucppublic/SLS

For USA, Canada, Pacific Rim, Asia and Latin America customers:

Machine name: sosco
Login name: uusls (fourth character is the letter "l")
No password

List of modems available for UUCP transfer from sosco:

V32, V32bis	+408 425-3502
Telebit Trailblazer	+408 429-1786

List of modems available for UUCP transfer from scolon.sco.com:

For SCO Online Support (SOS) BBS download:

These supplements can be downloaded interactively via XMODEM, YMODEM, ZMODEM or Kermit. Follow the menu selections under "Toolchest" from the main SOS menu.

List of modems available for interactive transfer from SOS:

V32, V32bis	+408 426-9495
Telebit Trailblazer	+408 426-9525

Note: telnet access to SOS is available by telneting to sos.sco.com

For customers with access to CompuServe:

Type "GO SCOFORUM"

For ftp via World Wide Web:

URL to open: ftp://www.sco.com

What to do once the files have been downloaded to the local machine

For SCO OpenServer 5.0.0 SLSs:

SCO OpenServer 5.0.0 SLS's usually consist of two phases: "Loading" and "Applying". The instructions that follow enable you to install the patch from the media image downloaded from this site.

NOTE: Steps 2-11 are documented in each SLSs associated coverletter.

1. Request the file(s) and cover letter/documentation via your favorite file transfer protocol. (Note: if transferring to a DOS based machine you will need to transfer the files to a SCO OpenServer 5.0.0 machine before proceeding to step 2)

2. Uncompress the media image(s), if necessary, by using the uncompress(C) command.

3. Copy the media image to the /tmp directory and name it VOL.000.000.

   NOTE: If the SLS contains more than one volume image, copy the first volume to VOL.000.000, copy the second volume to VOL.001.000, and so on until all volumes have been copied.

4. Execute the command:

   ```
   scoadmin software
   ```
   or double click on the Software Manager icon on the desktop

5. Pull down the "Software" menu and select "Patch Management-->Load Patch".

6. You will see the "Begin Load Patch" menu. Be sure the local machine name is selected and choose "Continue".

7. You will see the "Select Media" menu.

8. Pull down the "Media Device" menu and select "Media Images", then choose "Continue". You will then see the "Enter Image Directory" menu. Enter /tmp and

choose "OK".

9. You will see the "Load Patch Preference" menu. Choose "Full".

10. You will see the "Load Patch Progress" window. If the patch loads successfully, you will see a "Message" window which states "Load Patch complete". Choose "OK". You are then returned to the main Software Manager window.

11. To apply the patch see step 2 under section II, "Applying the Patch" located in the SLS' associated cover letter.

For SCO UNIX, ODT and XENIX:

The files ending in .Z have been reduced in size using the compress utility. These files must first be unpacked using uncompress(C). Files ending in .ltr or .doc are cover letters and installation instructions for the corresponding supplements. The cover letters assume you have received the supplements on diskette. To install a supplement, you must first transfer it to a diskette using the following procedure:

1. Request the file and cover letter/documentation via your favorite file transfer protocol. (Note: if transferring to a DOS based machine you will need to transfer the files to a SCO UNIX machine before proceeding to step 2)

2. Unpack the file as necessary using compress(C).

3. Use the dd(C) command to transfer the supplement file to the diskette. For example, if the supplement file is "uod001.n1" and is in the /usr/spool/uucppublic directory on your system, and the diskette is 3.5-inch, 720k, the command would be:

```
dd if=/usr/spool/uucppublic/uod001.n1 of=/dev/fd0135ds9
```

   Substitute the appropriate device name for "/dev/fd0135ds9" if transferring to a diskette of another capacity. The diskette must be formatted using the format(C) command before the data can be transferred.

4. Follow the installation instructions given in the cover letter or documentation file.

For SCO UnixWare:

Follow the instructions located in the associated text file for each supplement.

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

VULNERABILITY	OPERATING SYSTEM PRODUCT	PATCH ID
at, login, prwarn, sadc,pt_chmod, passwd, ex, vi, view, vedit, etc COMMANDS	UNIX SYSTEM v/386 r3.2 v4.0,1,2 OPEN DESKTOP r2.0, 3.0 OPEN SERVER NETWORK 3.0 OPEN SERVER ENTERPRISE 3.0	SLS/uod392b
KERNEL SECURITY	OPEN SERVER 5, 5.0.2 INTERNET FASTSTART 1.0	SLS/oss436a
RPC.MOUNTD	UNIX SYSTEM V/386 r3.2 v4.2 OPEN DESKTOP 3.0 OPEN SERVER NETWORK 3.0 OPEN SERVER ENTERPRISE 3.0	SLS/net398b
SENDMAIL	UNIX SYSTEM V/386 r3.2 v4.2 OPEN DESKTOP 3.0 OPEN SERVER NETWORK 3.0 OPEN SERVER ENTERPRISE 3.0	SLS/net382e☞
SENDMAIL	INTERNET FASTSTART 1.0.0 OPEN SERVER 5.0.0,2	SLS/oss443a
XTERM LOGGING	OPEN DESKTOP 2.0, 3.0	SLS/oda377a
PASSWD COMMAND	UNIX SYSTEM V/386 r3.2 v2.0, 4.0, 4.2 OPEN DESKTOP 1.1, 2.0, 3.0	SLS/uod368b
FILE PERMISSIONS	UNIX SYSTEM V/386 r3.2 v4.2 OPEN DESKTOP 3.0	SLS/uod380b
SYSTEM CALLS	UNIXWARE 2.1.0	PTF 3063

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

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

SYSTEM CALLS in UNIXWARE 2.0.x

Some system calls in the SCO UnixWare 2.0 environment will allow a local user to gain higher privileges than what is authorized. To fix the problem, do the following as root:

```
/etc/conf/bin/idtune -f RSTCHOWN 1
/etc/conf/bin/idbuild -B
init 6
```

SCO has provided a (T)echnical (L)ibrary (S)upplement which contains publicly available security tools such as tcp_wrappers, md5, lsof, COPS, etc., in both source and binary form. This library is available at ftp.sco.COM /TLS