SILICON GRAPHICS PLATFORM SPECIFIC SECURITY PATCHES

This appendix deals with vendor-provided patches that **MUST** be installed to properly secure a SGI IRIX Unix system. When SGI is informed of or discovers a vulnerability, they will issue a Security Advisory concerning the defect in the software product. The bulletin will contain a patch identification number that can be retrieved to correct the defect. Patches can be directly obtained from a SGI ftp site "sgigate.sgi.com" in the ~ftp/Security directory.

Patches for operating systems 5.2 and above are install images and require the patch-aware installation program /usr/sbin/inst. If this program is not existent on your system, it can be obtained via patch #84.

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

VULNERABILITY	OPERATING SYSTEM	PATCH ID
PRINTER TOOL	IRIX 5.2, 6.0, 6.01	#65
RDIST	IRIX 5.2	#130
CLOGIN/SGIHELP	IRIX 5.2	#65
LPR	IRIX 5.2	#131
MSDOSD	IRIX 5.2, 6.0, 6.01	#167
SENDMAIL	IRIX 5.2, 5.3, 6.0, 6.01	#526 & #1146
LIBCADMIN	IRIX 5.2, 6.0	#211
GUI PERMS TOOL	IRIX 5.2, 6.0, 6.01	#373
SYSLOGD	IRIX 5.2, 5.3, 6.0, 6.01, 6.1	#1146
TELNETD	IRIX 5.2, 5.3, 6.0,6.01	#1020
OBJECT SERVER	IRIX 5.2, 6.0	#1052
SENDMAIL	IRIX 6.1	#1146
RPC.STATD	IRIX 5.2	#1145
RPC.STATD	IRIX 5.3, 6.0, 6.01	#1128
TELNETD	IRIX 6.1	#1010
OBJECT SERVER	IRIX 5.3	#1096
OBJECT SERVER	IRIX 6.01	#1151
OBJECT SERVER	IRIX 6.1	#1090
GUI PERMS TOOL	IRIX 5.3	#1324
GUI PERMS TOOL	IRIX 6.1	#1325
GUI PERMS TOOL	IRIX 6.2	#1326
RDIST	IRIX 6.0	#90
LPR	IRIX 6.0	#91
LIBCADMIN	IRIX 6.01	#212
DESKTOP 5.3	IRIX 5.2	#65 & #1519
DESKTOP 5.3	IRIX 5.3	#1518
DESKTOP 5.3	IRIX 6.1	#1517

VULNERABILITY	OPERATING SYSTEM	PATCH ID
DESKTOP 5.3	IRIX 6.2	#1516
SYSTEM MONITOR	IRIX 5.3, 6.1	#1110
SYSTEM MONITOR	IRIX 6.2	#1417
SYN FLOOD/PING ATTACK	IRIX 5.3	#1529
SYN FLOOD/PING ATTACK	IRIX 6.2	#1418
NETPRINT	IRIX 5.3, 6.1	#1685
NETPRINT	IRIX 6.2	#1686
XFS FILESYSTEM	IRIX 5.3	#1409
XFS FILESYSTEM	IRIX 6.1	#1674
XFS FILESYSTEM	IRIX 6.2	#1667
SEARCHBOOK	IRIX 5.2	#1595
SEARCHBOOK	IRIX 5.3	#1596
SEARCHBOOK	IRIX 6.1	#1597
SEARCHBOOK	IRIX 6.2	#1598

In addition to the patches listed above, the following issues pertinent to an IRIX environment **MUST** be addressed to properly secure the system.

ATT Packaging Utility for IRIX Systems

There is a vulnerability present in this subsystem that affects IRIX 5.2, 5.3, 6.0, 6.01, and 6.1 which will allow a user to gain unauthorized authority on the system.

To verify if the subsystem is installed, issue the following command:

```
versions eoe2.sw.oampkg | grep oampkg
```

If the subsystem is installed, issue the following commands as root to secure the environment:

```
chmod 755 /usr/pkg/bin/pkgadjust
chmod 755 /usr/pkg/bin/abspath
```

OutOfBox and Systour Packages for IRIX Systems

There is a vulnerability present in these subsystems that affect IRIX 5.x, 6.0, 6.01, 6.1, 6.2, and 6.3 which will allow a user to gain unauthorized authority on the system.

To verify if the subsystems are installed, issue the following command:

```
versions OutOfBox.sw systour.sw
I = Installed   R=Removed
```

If no output is returned by the command, the subsystems are not installed and no further action is necessary.

To remove the setuid permissions on the programs, execute:

```
chmod u-s /usr/lib/tour/bin/RemoveSystemTour
chmod u-s /usr/people/touur/oob/bin/oobversions
```

To remove the vulnerable subsystems entirely, execute:

```
versions -v remove systour OutOfBox
```

IRIX 6.3 does not have the tour subsystem but does have OutOfBox

To remove the setuid permissions on the programs, execute:

```
chmod u-s /usr/people/touur/oob/bin/oobversions
```

To remove the vulnerable subsystems entirely, execute:

```
versions -v remove OutOfBox
```