SCO OpenServer Release 5.0.7 Maintenance Pack 5 Release and Installation Notes

The SCO OpenServer(TM) Maintenance Pack 5 contains important fixes for your SCO OpenServer Release 5.0.7 system and should be applied at your next maintenance period.

NOTE: Maintenance Pack 5 is the fourth in the series of Maintenance Packs provided for SCO OpenServer Release 5.0.7. Because the previous Maintenance Pack was coordinated with the release of Update Pack 3, there was no Maintenance Pack 2.

These *Release and Installation Notes* contain critical information that you need to know before and after installing SCO OpenServer Release 5.0.7 Maintenance Pack 5. Please familiarize yourself with the information that is relevant to your system, then install the Maintenance Pack according to the instructions in this document.

NOTE: Unless otherwise noted, this document supplements the SCO OpenServer Release 5.0.7 *Late News*, which are still relevant. As information becomes available after the publication of these *Release and Installation Notes*, it is added to the SCO OpenServer Release 5.0.7 *Late News* document, available from the SCO web site at:

http://www.sco.com/support/docs/openserver

These *Release and Installation Notes* cover the following topics:

About Maintenance Packs and Update Packs

Historically, there were two support ``tracks'' that were available to SCO OpenServer Release 5.0.7 customers:

Maintenance Packs

A Maintenance Pack (MP) is a collection of security updates and fixes for reported problems. Maintenance Packs are made available periodically and can be downloaded and installed free-of-charge. Maintenance Packs are cumulative, so only the latest one needs to be installed.

Update Packs

An Update Pack (UP) is a collection of some of the new features and product enhancements that will be included in the next SCO OpenServer release. Available only for registered subscribers to the SCO Update Service, Update Packs provide a simplified and streamlined process for deploying new technology and keeping systems updated.

As of Maintenance Pack 4, the SCO OpenServer Release 5.0.7 Update Pack track was discontinued and new licenses are no longer available. All of the functionality from the Update Packs is included in Maintenance Pack 5.

Obtaining Maintenance Packs

SCO OpenServer Maintenance Pack 5 is available for download from the SCO OpenServer Release 5.0.7 Supplements web page:

http://www.sco.com/support/update/download/osr507list.html

Additionally, SCO OpenServer Maintenance Pack 5 is included on the SCO OpenServer Release 5.0.7 Supplement CD Version 5. The SCO OpenServer Release 5.0.7 Supplement CD also provides other new and updated components, including Java 2 SE 1.4.2, Samba, Squid, and updated graphics, NIC, and HBA drivers. Your SCO OpenServer media kit may contain Version 5 of the Supplement CD; if not, you can download the ISO image for this CD from the SCO OpenServer Release 5.0.7 Supplements web page.

Before installing the Maintenance Pack from the Supplement CD, check the SCO OpenServer Release 5.0.7 Supplements web page to verify that the Supplement CD contains the most current Maintenance Pack available.

Before installing the Maintenance Pack

Before installing SCO OpenServer Release 5.0.7 Maintenance Pack 5, note the following:

- Back up the data on your system and verify the integrity of the backup.
- To prevent the possibility of introducing software conflicts on your system, you are strongly encouraged to install the entire Maintenance Pack. At a minimum, you **must** install the following components from Maintenance Pack 5:
    - the RS507D Release Supplement -- a critical requirement for the other components in the Maintenance Pack to function correctly.

    - the Perl package and the Supplemental Graphics, Web, and X11 Libraries (GWXLIBS) package -- several other packages, such as Apache and OpenSSH, depend on these libraries and will fail with dynamic linker errors if they are not present.
    - any component of the Maintenance Pack that updates existing software (expand the Maintenance Pack in **custom** to view the list of components).
- Maintenance Pack 5 can only be installed on SCO OpenServer Release 5.0.7 systems.
- Maintenance Pack 5 supersedes the following Supplements:
    - SLS OSS631 -- Supplemental Graphics, Web, and X11 Libraries
    - SLS OSS646 -- Execution Environment Supplement
    - SLS OSS656 -- Licensing Update
    - SLS OSS662 -- MP1 Supplement
    - SLS OSS669 -- Socket Driver Supplement
    - SLS OSS671 -- setclk Supplement
    - Large Filesystem Performance Supplement (lpfs)
    - **wd** Driver Supplement

NOTE: It is not necessary to remove any of the supplements listed above before installing Maintenance Pack 5, but **do not install any of these supplements** on your system after you have installed MP5.

- Before installing the Maintenance Pack, you should remove OSS646A/OSS646B and OSS656A/OSS656B. When you remove these supplements, you do not need to reboot the system after the kernel is re-linked. The Maintenance Pack installation also re-links the kernel -- you can reboot at that point.
- **Do not** install any of the other products provided on the SCO OpenServer Release 5.0.7 Supplement CD Version 5 until you have first installed Maintenance Pack 5. See */info/readme.htm* on the Supplement CD for information on issues that affect the order in which certain products on the CD should be installed.

wd driver BTLD and the Symmetrical Multiprocessing product (SMP)

When performing an ISL using the new wd driver BTLD from the Supplement 5 CD, the system may panic when rebooting after loading the SMP product (without MP5 installled):

```
WARNING: hd: no root disk controller was found
```

- If you are going to use the new wd driver BTLD at ISL and you plan on installing SMP, you should install MP5 right after installing SMP without rebooting first.
- If you have installed SMP after MP5, simply re-install MP5 before rebooting.

Maintenance Pack Installation

NOTE: Be sure to read ``Before installing the Maintenance Pack'' prior to starting this procedure.

You can acquire and install SCO OpenServer Release 5.0.7 Maintenance Pack 5:

- directly over the Internet using the SCO Update function in the **Software Manager**.
- by downloading the MP media images from either the SCO web site or FTP site.
- from the SCO OpenServer Release 5.0.7 Supplement CD Version 5.

If there are multiple systems on your TCP/IP network that require Maintenance Pack 5, you can load and install the MP on a software server and use it as a centralized distribution point. See ``Installing the Maintenance Pack across the network'' for more information.

Installing the Maintenance Pack using SCO Update

SCO Update allows you to install Maintenance Packs directly over the Internet. This approach saves you the time -- and extra hard disk space -- of first downloading installable image files from the SCO web or FTP sites.

NOTE: Maintenance Pack 1 added support for SCO Update to the **Software Manager**. If none of the previous Maintenance Packs (1-4) were installed on your system, SCO Update will not be available from within the **Software Manager** until after you install MP5.

NOTE: You will not be able to use the SCO Update feature if you are behind a firewall that prevents incoming FTP connections (i.e., the use of passive FTP is required). If you try to connect to the SCO Update server in this situation, the **Software Manager** displays the following timeout message after a few minutes:

```
Unable to initialize device
```

A fix for this problem will be made available in a future supplement or release.

To use SCO Update:

1. Log in as *root*.
2. Start the **Software Manager** by double-clicking on its icon on the desktop, or by entering the following at the command-line prompt:
   scoadmin software
3. From the **Software** menu, select **SCO Update**. The system connects to the SCO Update server.

   The **Install Selection** window displays all of the SCO OpenServer Release 5.0.7 maintenance packs, drivers, and so forth that are currently available.

4. Highlight Maintenance Pack 5 and click on **Install**.

   The selected software is automatically downloaded and installed on your system.

WARNING: The **Software Manager** displays one or more warnings if the Maintenance Pack contains fixes for software features that are not currently installed on your system. If you do not plan to install the affected package (for example, SMP), you can ignore such messages and click on **Continue**. However, if you do plan to install this package later, you should stop the install process now by clicking on **Cancel**, install the package in question from the installation media, and restart the Maintenance Pack installation. This ensures the fixes are applied properly (and avoids potential problems).

If any Maintenance Pack fixes were not installed because the corresponding feature was not present, the **Software Manager** shows the Maintenance Pack as only partially installed. This is normal.

---

5. When the installation is complete, click on **OK**.
6. Exit the **Software Manager** by selecting the **Host** menu, then **Exit**.
7. Reboot the machine. (Because the **Software Manager** relinks the kernel, you must reboot before the new kernel takes effect.)

We recommend that you use SCO Update periodically to check for new updates, fixes, or drivers for SCO OpenServer Release 5.0.7.

Installing the Maintenance Pack from downloaded media images

To install the SCO OpenServer Release 5.0.7 Maintenance Pack 5 from media images that you manually download:

1. Log in as *root*.

2. Download the Maintenance Pack from either the SCO web site or using FTP:
   - to use the web, go to the SCO OpenServer Release 5.0.7 Supplement web page:
     http://www.sco.com/support/update/download/osr507list.html
   - to use FTP, go to the SCO Support Download Area for SCO OpenServer Release 5.0.7 Maintenance Pack 5:
     ftp://ftp.sco.com/pub/openserver5/507/mp/osr507mp5

NOTE: Maintenance Pack 5 consists of a tar archive containing a number of media image files with names of the form *VOL.000.000*, *VOL.000.001*, and so forth. Because all maintenance packs use this same filename scheme, you should create a master directory with a unique subdirectory to store each pack. The master directory could be */usr/updates*, */usr/spool/patches*, or whatever suits your system layout. The master hierarchy should be writable by *root* only.

---

3. Download the *osr507mp5_vol.tar* file and use this command to extract the media image files:
   tar xvf osr507mp5_vol.tar
4. Start the **Software Manager** by double-clicking on its icon on the desktop, or by entering the following at the command-line prompt:
   scoadmin software
5. From the **Software** menu, select **Install New**.
6. When prompted for the host (machine), select the current host and then click on **Continue**.
7. Select **Media Images** as the Media Device, then click on **Continue**. (You may need to scroll down before you see the **Media Images** option.)
8. Enter the absolute pathname for the directory that contains the Maintenance Pack 5 media images. For example:
   /usr/spool/patches/osr507mp5

   Click on **OK**.

9. In the **Install Selection** window, make sure that the Maintenance Pack is highlighted, then click on **Install**.

NOTE: Any component of the Maintenance Pack that updates existing software (such as the RS507C Release Supplement) **must** be installed. New features are optional.

10. If you previously installed any of the components that are modified by the Maintenance Pack, you are notified that these components will be upgraded. Click on **Continue**.

    Additionally, you are warned if certain packages in the Maintenance Pack will not be installed because the software they modify is not installed on your system. Click on **Continue**.

    WARNING: The **Software Manager** displays one or more warnings if the Maintenance Pack contains fixes for software features that are not currently installed on your system. If you do not plan to install the affected package (for example, SMP), you can ignore such messages and click on **Continue**. However, if you do plan to install this package later, you should stop the install process now by clicking on **Cancel**, install the package in question from the installation media, and restart the Maintenance Pack installation. This ensures the fixes are applied properly (and avoids potential problems).

    If any Maintenance Pack fixes were not installed because the corresponding feature was not present, the **Software Manager** shows the Maintenance Pack as only partially installed. This is normal.

---

11. When the installation is complete, click on **OK**. The **Software Manager** lists Maintenance Pack 5 among the installed software.
12. Exit the **Software Manager** by selecting the **Host** menu, then **Exit**.
13. Reboot the machine. (Because the **Software Manager** relinks the kernel, you must reboot before the new kernel takes effect.)

Installing the Maintenance Pack from CD-ROM

The SCO OpenServer Release 5.0.7 Maintenance Pack 5 is included on the SCO OpenServer Release 5.0.7 Supplement CD Version 5. Your SCO OpenServer media kit may contain Version 5 of the Supplement CD; if not, you can download the ISO image for this CD from the SCO OpenServer Release 5.0.7 Supplements web page.

To install the SCO OpenServer Release 5.0.7 Maintenance Pack 5 from the SCO OpenServer Release 5.0.7 Supplement CD Version 5:

1. Log in as *root*.
2. Insert the SCO OpenServer Release 5.0.7 Supplement CD Version 5 into the drive.

3. Start the **Software Manager** by double-clicking on its icon on the desktop, or by entering the following at the command-line prompt:
   scoadmin software
4. From the **Software** menu, select **Install New**.
5. When prompted for the host (machine), select the current host and then click on **Continue**.
6. Select the appropriate CD-ROM drive as the Media Device, then click on **Continue**.
7. In the **Install Selection** window, make sure that the Maintenance Pack is highlighted, then click on **Install**.

NOTE: Any component of the Maintenance Pack that updates existing software (such as the RS507D Release Supplement) **must** be installed. New features are optional.

---

8. If you previously installed any of the components that are modified by the Maintenance Pack, you are notified that these components will be upgraded. Click on **Continue**.

WARNING: The **Software Manager** displays one or more warnings if the Maintenance Pack contains fixes for software features that are not currently installed on your system. If you do not plan to install the affected package (for example, SMP), you can ignore such messages and click on **Continue**. However, if you do plan to install this package later, you should stop the install process now by clicking on **Cancel**, install the package in question from the installation media, and restart the Maintenance Pack installation. This ensures the fixes are applied properly (and avoids potential problems).

If any Maintenance Pack fixes were not installed because the corresponding feature was not present, the **Software Manager** shows the Maintenance Pack as only partially installed. This is normal.

---

9. When the installation is complete, click on **OK**. The **Software Manager** lists Maintenance Pack 5 among the installed software.
10. Exit the **Software Manager** by selecting the **Host** menu, then **Exit**.
11. Reboot the machine. (Because the **Software Manager** relinks the kernel, you must reboot before the new kernel takes effect.)

Installing the Maintenance Pack across the network

You can install SCO OpenServer Release 5.0.7 Maintenance Pack 5 from one SCO OpenServer Release 5.0.7 system onto another across a TCP/IP network. To do so, you need a software server, which you can create as described in ``Installing and managing software over the network'' in the *SCO OpenServer Networking Guide*. This server has a user account called *swadmin*.

Install or load Maintenance Pack 5 on the software server using one of the installation procedures described in ``Maintenance Pack Installation''. Also see ``Installing and managing software components'' in the *SCO OpenServer Handbook* for more information on loading software.

To install Maintenance Pack 5 onto a local machine once the Maintenance Pack is available from the software server, start the **Software Manager** and select **Install New**. In the **Begin Installation** window, you are prompted for the source location of the Maintenance Pack. Select **From Another Host**. You need to provide the name of the software server, as well as the password of the *swadmin* user on the software server.

Removing a Maintenance Pack

WARNING: Because of interdependencies between the components that are included in Maintenance Packs, partial removal of an MP is not supported.

Removing Maintenance Pack 5 de-installs the Apache, Mozilla, OpenSSH, Perl, and Supplemental Graphics, Web, and X11 Libraries (GWXLIBS) components. When these components are removed, many system functions will cease to work, including Squid, Samba, and the GNU Development Tools (if installed).

After removing the Maintenance Pack, it is imperative that you re-install the previous versions of Apache, Mozilla, OpenSSH, Perl, and Supplemental Graphics, Web, and GWXLIBS. This section explains how to do this.

To remove the Maintenance Pack and reinstall your previous versions of the Apache, Mozilla, OpenSSH, Perl, and GWXLIBS components:

1. Log in as *root*.
2. Start the **Software Manager** by double-clicking its icon on the desktop, or by entering the following at the command-line prompt:
   scoadmin software
3. Select the Maintenance Pack in the list of installed software.
4. From the **Software** menu, select **Remove Software**. In the confirmation window, verify that you selected the correct software, then click on **Remove**.

5. A window displays, showing you a list of software that will stop functioning after the Maintenance Pack is removed. Click on **Continue**.
6. When the **Removal complete** window appears, click on **OK** and exit the **Software Manager** by selecting **Exit** from the **Host** menu.
7. Now re-install Apache, Mozilla, OpenSSH, Perl, and GWXLIBS. It is important that you replace these components with the versions that you were running prior to installing Maintenance Pack 5. If your system contains Maintenance Pack 4, use that media.
8. Restart the **Software Manager**, as you did in Step 2.
9. From the **Software** menu, select **Install New**.
10. When prompted for the host (machine), select the current host and then click on **Continue**.
11. Select the appropriate CD-ROM drive as the Media Device, then click on **Continue**.
12. Depending on the media you are using, the list displayed in the **Install selection** window will be different. Double-click on the appropriate software -- maintenance pack or operating system edition. From the expanded list, select to install the Apache, Mozilla, Secure Shell (OpenSSH), Perl, and Supplemental Graphics, Web, and X11 Libraries components. You can use the <Ctrl> key to select multiple components for installation. When all of these components are highlighted, click on **Install**.
13. When the installation is complete, click on **OK**.
14. Exit the **Software Manager** by selecting the **Host** menu, then **Exit**.
15. Reboot the machine. (Because the **Software Manager** relinks the kernel, you must reboot before the new kernel takes effect.)

Highlights of the Maintenance Pack

Changes and additions provided by this Maintenance Pack include:

- enhanced USB support
- Support for enhanced mode controllers
- support for IDE hard disks larger than 137GB
- Hyper-Threading Technology and multi-core support
- cdrtools
- multisession CD read support
- DVD writing with dvdrecord
- updates to the Supplemental Graphics, Web, and X11 Libraries
- updates to X.Org X11 runtime libraries and core fonts
- updates to Perl
- updates to OpenSSH
- updates to the Apache Web Server
- additions to Internet Services: Tomcat and JK
- updates to Mozilla web browser and new plugin support

- Lynx web browser
- updates to MMDF
- CUPS printer subsystem
- GIMP-print support
- ESP Ghostscript
- Foomatic printer drivers
- extended shells
- Vim text editor
- updates to UDK compatibility libraries

NOTE: Drivers for new hardware have been moved out of the Maintenance Packs and are now available on the Supplement CD.

Enhanced USB support

Maintenance Pack 5 includes an enhanced USB driver that supports both USB modems and serial adapters. The driver adds support for USB modems that conform to the CDC/ACM specification. Written to the to the Uniform Driver Interface (UDI) specification, the new driver includes a number of fixes that improve performance and device support. In addition:

- The **giomap_noded**(ADM) utility now manages device nodes for USB serial devices. **giomap_noded** also creates links in */dev/usb* for each host controller instance (HCI) detected. These links are named **usbprobe#**.
- The **usbprobe**(ADM) utility now handles multiple HCIs. The **usbprobe -A** command finds all sequentially enumerated HCIs and displays the devices attached.

Support for enhanced mode disk controllers

Maintenance Pack 5 includes a modified **wd** driver. The **wd** driver (ATA and ATAPI devices) has been modified to support "enhanced mode" controllers. Legacy controllers appear as a "primary" or "secondary" with the original ISA hardware parameters assigned to those devices, while enhanced controllers appears as a PCI device. (Some chipsets present one or two of their controllers as *both* legacy and enhanced controllers; the OS treats these devices as traditional primary or secondary controllers.)

This enhancement allows the use of more than two ATA controllers. To avoid renumbering controllers on installed systems, the legacy primary controller is always controller 0 (regardless of whether the controller exists or has any devices attached to it). The secondary controller and any enhanced mode controllers are counted only if they have at least one device attached. (As with legacy controllers, enhanced controllers support two devices). Thus, on a system without a legacy secondary controller (or a legacy secondary controller without attached devices), the first enhanced mode controller

is controller 1 (sometimes referred to as the secondary controller by the operating system).

This affects the install process, which allows the selection of an ATAPI CD-ROM only on the primary or secondary controller. On some motherboards with SATA (serial ATA) ports, all of the SATA ports are on the enhanced controllers. To install from a SATA CD-ROM attached to such a system, the wd BTLD must be used. In addition, the CD-ROM must be plugged into one of the SATA ports on the *first* SATA controller. Furthermore, if the motherboard has a secondary controller, it must have no devices attached. This enables the SATA CD-ROM to appear as though it is attached to the secondary controller.

Device access

As in previous releases, ATA hard drives are enumerated in order of discovery. The only difference is that more than four drives are supported. ATAPI devices use explicit controller and master/slave numbers. (The controller numbering is described above.) The difference with past operation is that controller numbers higher than 1 are supported. (As in the past, ATAPI devices use PIO mode.)

Support for IDE hard disks larger than 137GB

This feature was originally provided in the Update Packs and then Maintenance Pack 3.

Maintenance Pack 5 includes a version of the **wd**(HW) driver that supports IDE hard disks larger than 137GB.

NOTE: If you are installing from scratch and you have a new IDE hard disk that is larger than 137GB that you want to add to your system, you should do so **after** you have installed the Maintenance Pack and the new **wd** driver. If you want to use the disk as your root drive, you need to load the new driver at boot time (using the **link**(HW) bootstring) before beginning the installation.

If your system currently uses an IDE drive larger than 137GB, the new **wd** driver makes it possible to use the full capacity of the disk. To use the entire disk, however, you must manually reconfigure the drive to recreate the existing disk partitions or to create new ones. The **wd** driver *readme* explains this process in detail.

Instructions for installing the **wd** driver are provided on the SCO web site at:

http://www.sco.com/support/update/download/wddrvr.html

or the SCO OpenServer Release 5.0.7 Supplement CD Version 5. **We strongly recommend that you review these instructions before using the new features of the driver.**

Hyper-Threading Technology and multi-core support

This feature was originally provided in the Update Packs and then Maintenance Pack 4.

Hyper-Threading allows two series of instructions to run simultaneously and independently on a single Intel® HT-enabled processor. With Hyper-Threading Technology enabled, the system treats a physical processor as two ``logical'' processors. Each logical processor is allocated a thread on which to work, as well as a share of execution resources such as cache memories, execution units, and buses.

Hyper-Threading Technology can be used on an SCO OpenServer Release 5.0.7 system that is equipped with the following:

- an Intel Xeon(TM) or HT-enabled Intel Pentium® 4 processor
- a chipset that supports HT Technology
- a system BIOS that supports HT Technology

NOTE: By default, Hyper-Threading support is disabled when Maintenance Pack 5 is installed. The Hyper-Threading support provided in Update Pack 3 was enabled by default. To enable Hyper-Threading support after Maintenance Pack 5 is installed, see the **hyperthread**(HW) manual page.

Multi-core support was first provided in Maintenance Pack 4. A multi-core processor is a single physical processor that includes two or more ``cores'' and one or more logical processors per core. Each core acts as a discrete processor, complete with its own set of execution resources. A **dual-core** processor includes two cores, with one logical processor per core. A dual-core processor that also includes Hyper-Threading Technology provides two cores and two logical processors per core, allowing the execution of four simultaneous threads.

Maintenance Pack 5 provides support for Intel Xeon and Intel Pentium 4 multi-core processors. SCO OpenServer multi-core support also requires a chipset and a system BIOS that support HT Technology.

NOTE: Hyper-Threading Technology and multi-core processor support for SCO OpenServer is provided by the SCO OpenServer Release 5.0.7 Symmetrical Multiprocessing (SMP) product. If you want Hyper-Threading Technology or multi-core support, the SMP product must be installed before Maintenance Pack 5.

An SMP license is not required to install SMP on a single-CPU system; simply select to *Defer* licensing during the installation.

For more details on Hyper-Threading and multi-core support in SCO OpenServer Release 5.0.7, see the **hyperthread**(HW) manual page.

CD writer support: cdrtools

First provided in Maintenance Pack 3.

The cdrtools package was updated to version 2.01.01a01 in Maintenance Pack 4. This package is a set of programs for creating CD images (**mkisofs**) and writing data to recordable/rewritable CDs (**cdrecord**).

The **cdrecord**(1) utility has been updated 2.11 in Maintenance Pack 5.

As of 2.01, **cdrecord**(1) was updated to check the CD recorders DMA (Direct Memory Access) speed and adjust the default burn rate accordingly. However, SCO OpenServer Release 5.0.7 does not currently support DMA mode for ATAPI devices; only PIO mode is used. Consequently, you may see a message similar to:

```
   cdrecord: DMA speed to slow (OK for 16x),  Cannot write at speed
24x.
```

This message is misleading because there is no performance degradation between this version of **cdrecord** and the version provided with Update Pack 3. CD recording continues to run in PIO mode -- a recording at 24x takes the same amount of time to complete as a recording at 16x speed.

ATAPI DMA support is planned for a future maintenance pack release.

cdrecord(1), a port of the ProDVD utility, supports many options and formats that are beyond the scope of basic file archiving. The following sections document the most common tasks for creating data CDs and include information specific to SCO OpenServer Release 5.0.7.

Tested hardware

The following drives have been tested on SCO OpenServer Release 5.0.7:

Matsushita CW-7502
Philips CDD-2600
Plextor PX-R412Ci
Plextor PX-R820Ti
Plextor PX-W2412TA

Plextor PX-W4824TA
Ricoh MP6200S
Teac CD-R50S
Teac CD-R55S
Teac CD-R56S
Teac CD-R58S
YAMAHA CDRW4416S
YAMAHA CRW2260

Most MMC-compliant CD writers should work.

Configuration

If you have not already used the CD drive to install SCO OpenServer Release 5.0.7, you need to manually configure the drive with the **mkdev cdrom** command.

Listing available devices

To display a list of CD devices on the system, use the **-scanbus** option of the **cdrecord**(1) command:

cdrecord -scanbus

A list of devices similar to this is displayed (SCSI addresses are shown regardless of the controller type):

```
scsibus0:
      0,0,0   0) 'ATAPI '  'CD-RW 52X24X ' 'MB51' Removable CD-ROM
      0,1,0   1) *
      0,2,0   2) *
      0,3,0   3) *
      0,4,0   4) *
      0,5,0   5) *
      0,6,0   6) *
      0,7,0   7) *
```

In this case an ATAPI CD writer is the first device on an IDE controller (address 0,0,0).

cdrecord default file (/etc/default/cdrecord)

This file contains the default device settings for **cdrecord**. First are the device, speed, and buffer settings (note that the latter two are commented out):

```
CDR_DEVICE=ide
#CDR_SPEED=40
#CDR_FIFOSIZE=4m
```

The CDR_DEVICE setting is actually an index into a table with a series of drive-specific defaults:

```
# drive name    device  speed   fifosize driveropts
#
teac=           1,3,0   -1      -1      ""
panasonic=      1,4,0   -1      -1      ""
plextor=        1,4,0   -1      -1      ""
sanyo=          1,4,0   -1      -1      burnfree
yamaha=         1,5,0   -1      -1      ""
ide=            0,0,0   -1      -1      burnfree
cdrom=          0,6,0   2       1m      ""
```

The default entry is **ide** (as defined by **CDR_DEVICE**). Because a generic SCSI driver is used for all CD drives, the SCSI address scheme (host adapter, device, LUN) is used even with IDE controllers. At the same time, this scheme only applies to IDE controllers with CD drives (that is, the numbering of host adapters is not absolute.) For example, on a system with no SCSI adapters and two IDE controllers, the controller with the CD drive attached is host adapter 0 (even if it happens to be the secondary IDE controller).

NOTE: On the command line, the LUN (0) can be omitted (as it is in the examples discussed here).

Note the default addresses for other drives are not realistic; be sure and change the device address in second column to match the actual drive settings. The other columns (speed, buffer size, and driver options) can be set as desired. A value of **-1** indicates that the device uses its own default value. The quotes in the column indicate an empty option list; **burnfree** allocates a larger buffer for write operations (if supported by the drive). Other options are documented in **cdrecord**(1).

Creating a data disc

Before using **cdrecord** to make a data disc, you must first create an ISO image with **mkisofs**. This sample command creates an ISO9660 image of the working directory (.) with Joliet (**-J**) and RockRidge (**-r**) directory entries and stores it in the file */tmp/cdimg.iso*:

mkisofs -r -J -o /tmp/cdimg.iso .

To write this image to a disc, you would use a command like this:

cdrecord -v -eject dev=0,0 /tmp/cdimg.iso

The **-v** is optional and generates verbose output. The **dev=** argument can also be omitted if the default drive is defined in */etc/default/cdrecord*. The **-eject** option ejects the disc when the process is complete. In addition, **cdrecord** displays a nine-second countdown to give you an opportunity to abort the command.

You can also perform a test burn using the **-dummy** option:

cdrecord -v -dummy /tmp/cdimg.iso

The command is executed as specified, but the laser is not activated.

NOTE: The **-dummy** option may actually damage media on certain older drives (rendering them unusable).

If the system is relatively idle (with little or no disk activity), it is possible to skip creating the image and pipe the output of **mkisofs** directly to **cdrecord**:

mkisofs -r /usr/home/cforbin | cdrecord -

In this example, the contents of */usr/home/cforbin* is written to the disc (the **-** argument takes data from the standard input).

WARNING: On active systems you should create an ISO image for best results.

Mounting a disc

You can mount and unmount a disc from the desktop using the **MountCD** icon, or from the command line as in these examples using */mnt* as a mount point:

mount -r /dev/cd0 /mnt
umount /mnt

Media support

cdrecord supports the following drive types/media:

Media Type	**Read-Write Behavior**
CD-R	Existing data cannot be erased or overwritten
	Additional sessions can be appended
CD-RW	Entire disc can be erased/blanked
	Explicit erasing/blanking required before rewrite
	Additional sessions can be appended

Multisession support

To create multisession disks, you must use the **-multi** option to leave the CD open (un-fixated) for writing additional sessions:

cdrecord -multi image.iso

To finalize a CD (making it non-writable), simply omit the **-multi** option.

Writing a new session on a CD normally hides the previous session from view (requiring an application that allows you to select the active session). However, it is possible to import the TOC (table of contents) from the previous session and make the previously-written data available in the ISO image for the new session.

In this example, **mkisofs** uses the **-C** option to execute the **cdrecord -msinfo** command on the specified drive (**-M 0,0**) to read the location of the previous session and uses the response to create the ISO image:

mkisofs -r -J -C `cdrecord -msinfo` -M 0,0 -o image.iso /usr/home/colossus

When **cdrecord** is used to write the image to CD, all the previous data will be accessible along with the new files (in this example, from */usr/home/colossus*).

Multisession support: mount(ADM)

First provided in Maintenance Pack 3.

The **mount**(ADM) command includes options to mount CD filesystems by session or sector. See the **mount**(ADM) manual page for details.

By default, the **mount**(ADM) command mounts the last session. To override the default and mount the first session, use the syntax in this example:

mount -o session=1 /dev/cd0 /mnt

At this time, only the first and last sessions can be mounted by session number. However, the **sector** option can be used to mount an arbitrary session by the starting sector number. On newer drives, you can use the **-toc** option of the **cdrecord**(1) command to obtain the starting sector:

cdrecord -toc

For a multi-session CD, the output looks something like this:

```
   track:   1 lba:         0 (        0) 00:02:00 adr: 1 control: 4
mode: 1
   track:   2 lba:     20235 (    80940) 04:31:60 adr: 1 control: 4
mode: 1
```

```
   track:   3 lba:     39262 (   157048) 08:45:37 adr: 1 control: 4
mode: 1
   track:lout lba:     53507 (   214028) 11:55:32 adr: 1 control: 4
mode: -1
```

You can use the lba output to mount the desired sector. In this example, the command mounts session 2, which starts at sector 20235:

mount -o sector=20235 /dev/cd0 /mnt

NOTE: If you used **cdrecord**(1) when it was provided on the Skunkware CD (and multisession CD read support was not present in SCO OpenServer Release 5.0.7), note that the the last session is now mounted by default. Multisession CDs typically include files from previous sessions by reference, so this should yield a better view of the contents of the disc.

DVD writing with dvdrecord

This feature was originally provided in the Update Packs and then Maintenance Pack 4.

This Maintenance Pack includes DVD writing support with the **dvdrecord**(C) command, a port of the **ProDVD** utility.

Because the industry standard for writing DVDs is SAO (DAO) mode, this is now the only mode supported by **dvdrecord**. The previously supported TAO and RAW modes are no longer available for writing DVDs.

NOTE: If you have not already used the DVD drive to install SCO OpenServer Release 5.0.7, you need to manually configure the drive with the **mkdev cdrom** command (which also supports DVD drives).

The command options for **dvdrecord** are the same as those for **cdrecord** (see ``CD writer support: cdrtools''). The **dvdrecord**(C) manual page is provided (and is maintained) by SCO. It contains basic information on creating DVD and CD data discs and includes key examples. The **cdrecord**(1) manual page is the generic documentation provided with the free software and is not specific to SCO UNIX operating systems. Refer to **cdrecord**(1) for the complete option set and information on creating specialized disc layouts and formats.

DVD writers tested

dvdrecord has been reported to work with most DVD drives. The following drives have been tested on SCO OpenServer Release 5.0.7:

- Pioneer DVR-A06
- Sony DWU-14A
- Plextor PX-708A

Updates to the Supplemental Graphics, Web, and X11 Libraries

First provided in Maintenance Pack 1.

Maintenance Pack 5 includes the following changes in the Supplemental Graphics, Web, and X11 Libraries (GWXLIBS):

- OpenSSL 0.9.7 updated to 0.9.7i
- OpenLDAP updated to 2.2.30
- GTK+ 2.x upgraded to 2.8.9
- ATK upgraded to 1.10.3
- Pango upgraded to 1.10.2
- glib 2.x upgraded to 2.8.4
- cURL upgraded to version 7.15.1
- librsvg upgraded to version 2.13.3 (now also builds the Mozilla SVG plugin if Mozilla is present)
- libgtkhtml upgraded to version 2.11.0
- libgsf upgraded to version 1.13.3
- Xalan upgraded to version 1.10.0
- readline upgraded to version 5.1
- lcms upgraded to version 1.15
- X.org libraries upgraded to version 6.9.0
- BerkeleyDB error fixed that prevented full paths being used for database names

Updates to X.Org X11 runtime libraries and core fonts

Maintenance Pack 5 updates the X.Org X11 runtime libraries, header files, and core fonts to Release 6.9.0. (As of Maintenace Pack 4, these libraries are now part of the Supplemental Graphics, Web, and X11 Libraries and no longer a separate package.)

The manual pages for the X.Org routines are also installed on the system, but are not included in the **MANPATH** environment variable. (This is done to avoid collision with the existing X11R5 man pages.) If you wish to access the X.Org manual pages instead of those for the X11R5 server, insert **/usr/X11R6/man** into your **MANPATH** variable (or the system-wide setting in */etc/default/man*) before the */usr/man* entry, as in this example:

```
MANPATH=scohelp:/usr/X11R6/man:/usr/man:/usr/gnu/man:/usr/local/man
```

If you add the X11R6 path to */etc/default/man*, you should also update the man page database by executing the following command as *root*:

/usr/man/bin/makewhatis /usr/X11R6/man/*

Updates to Perl

The Perl component has been updated to 5.8.8 in Maintenance Pack 5. This updated version includes a number of upgraded Perl modules. In addition, this version of Perl was recompiled to take advantage of the updated GWXLIBS component.

Updates to OpenSSH

OpenSSH has been updated to 4.3p2 in Maintenance Pack 5.

As of version 4.2p1, long passwords (longer than eight characters) are now supported. Previously, only the first eight characters of a password were recognized.

Note that if your SCO OpenServer system was installed with either the Low or Traditional security profiles, you need to activate the OpenSSH long password support. To do this, run the following command:

usermod -D -x "{passwdSignificantSegments 2}" <*username*>

Updates to the Apache Web Server

Maintenance Pack 5 includes the following changes to the Apache Web Server component:

- Apache Web Server updated to version 1.3.36
- PHP updated to version 4.4.2
- **mod_ssl** updated to version 2.8.27

Additions to Internet Services: Tomcat and JK

First provided in Maintenance Pack 3. There are no changes in Maintenance Pack 5.

The following Internet Services are included:

- Apache Tomcat Servlet Container 4.1.31: an open source package that provides a container for JavaServer Pages(TM) and Java(TM) Servlets. Requires the Java 2 JRE and Java SDK (1.4.2).
- JK: a plugin that replaces mod_jserv and handles the communication between Tomcat and Apache.

Consult the DocView Internet Services page for documentation links relating to these packages.

Tomcat notes

The following sections include additional information about Tomcat.

Enabling Tomcat

After installing Tomcat, you must enable it manually. To enable and start Tomcat, run these commands:

/etc/init.d/tomcat enable

When enabled, Tomcat also automatically restarts each time the system is rebooted.

Tomcat web application

After startup, the default web applications included with Tomcat are available by browsing:

http://localhost:8080/

The administrator application is available directly at:

http://localhost:8080/admin/login.jsp

The logins for the *admin* and other roles must be set up as described in the next section.

Using the Tomcat admin and manager logins

By default the *admin* and *manager* web logins are not enabled. To add these logins, do the following:

1. Edit the configuration file */usr/lib/apache/tomcat/conf/tomcat-users.xml*. The contents are similar to the following:

```
<tomcat-users>
<user name="tomcat" password="tomcat" roles="tomcat" />
<user name="role1"  password="tomcat" roles="role1"  />
<user name="both"   password="tomcat" roles="tomcat,role1" />
</tomcat-users>
```

2. You can change these entries to include the desired web login, password, and the role to which you want them assigned. (Do not confuse these "web" logins that are used to access the administrative web application with operating system system logins.) The *admin* and *manager* roles/logins allow someone with the proper password to run the **admin** and **manager** web applications. For example, the following entries create *admin* and *manager* web logins with **tomcat** as the password:

```
<role rolename="admin"/>
<role rolename="manager"/>
<user username="admin" password="tomcat" roles="admin"/>
<user username="manager" password="tomcat" roles="manager"/>
```

3. After making changes or additions, you must restart Tomcat:

   /etc/init.d/tomcat restart

Tomcat web application Java exception error

If you log into the Tomcat Application Manager, stop an Application, restart it, then proceed to the application path and then use the Back button to return to the Tomcat Web Application Manager, the following error may be displayed in the Messages box of the Tomcat Application Manager:

```
FAIL - Application at context path /tomcat-docs could not be started
FAIL - Encountered exceptionjava.lang.IllegalStateException:
standardHost.start /tomcat-docs: LifecycleException:  Container
StandardContext[/tomcat-docs] has already been started
```

This is not a fatal error and is not unique to SCO OpenServer Release 5.0.7 systems. The workaround is to use reload instead of stop or start.

Updates to Mozilla web browser and plugins

First provided in Maintenance Pack 3.

Maintenance Pack 5 updates the Mozilla web browser to version 1.7.13.

MozPlugger 1.7.3 replaced the Plugger 5.0 plugin that was provided in Maintenance Pack 3. MozPlugger is a general purpose multimedia plugin for Mozilla that supports the display of media files within the browser.

MozPlugger is configured to use **xpdf** 3.0.1 (also provided in Maintenance Pack 5) to display PDF documents in Mozilla. Additionally, Mozilla is pre-configured to work with the Java plugin provided on the SCO OpenServer Release 5.0.7 Supplement CD Version 5.

The SCO OpenServer Release 5.0.7 Skunkware Download area contains many packages providing multimedia support that can be configured in MozPlugger.

Mozilla and the XSENDER command

As of 1.7.12, Mozilla is configured to enable mail authentication via the **XSENDER** command. If your POP server does not support the **XSENDER** command and you wish to disable this feature, either edit the system-wide preferences in */usr/lib/mozilla-1.7.13/defaults/pref/mailnews.js* and set the **auth_login** preferences to ``false'', or add such entries to your individual Mozilla preferences as described at the following URL:

http://www.mozilla.org/unix/customizing.html#prefs

Lynx web browser

Maintenance Pack 5 includes version 2.85rel5 of Lynx, the character-based web browser. You can find documentation on the web at:

http://lynx.isc.org/lynx2.8.5/lynx2-8-5/lynx_help/lynx_help_main.html

Updates to MMDF

First provided in Maintenance Pack 3.

The following sections detail various updates and fixes made to MMDF.

Security fixes

Various buffer overflows, null dereferences, and core dumps that affect all MMDF binaries have been corrected. All but one of the MMDF binaries that were setuid root are no longer (they have been improved to make this unnecessary), reducing the potential for further exploitation. The local channel delivery program is still setuid root because it must deliver mail into users' mailboxes and run processes with users' UIDs.

Improvements to mmdftailor(F)

Three new MMDF general configuration parameters can be set in */usr/mmdf/mmdftailor*: **ORPHANAGE**, **DEADLETTER**, and **TAGCHARS**. See **mmdftailor**(F) for more information.

Improvements to submit(ADM)

Several changes have been made to **submit**(ADM):

- Messages can now be submitted with a null return address in protocol mode. Formerly, a null address for either the return address or a recipient address resulted in the silent termination of address-list processing. Address-list parsing is now terminated only by a **!**, as per the submit specification.
- Messages with a null return address that bounce are discarded instead of being sent to the orphanage.
- When messages are submitted with the do-not-return (**q**) option, a return address is no longer passed to remote hosts, preventing bounce messages from being generated.
- **relay** authorization now correctly interprets aliases that point offsite, include the addresses of users who have a *.forward* file that points offsite, as still being local addresses.
- There is now a "magic" address (**@@**) which is like any other bad address except that if it occurs in a *.forward* file or alias no complaint to **supportaddr** is issued. This can be used to prevent mail from being accepted for certain users, similar to

aliasing such users to a nonexistent address but without the notification that is generated every time a true bad address is referenced. An alias to **@@** can itself be used in aliases without generating warning mail, so that an alias like this can be set up:

```
@@: nosuchuser
```

Then the less cryptic address *nosuchuser* can be used in aliases and *.forward* files.

- Formerly, if **-t** ("trust me") was given to submit but the user was not a trusted user, a Source-Info line was added. Now in that case a Source-Info line is added only if the user is not who they claim to be in the most authoritative From/Sender field. For the purpose of this test, a plain Sender is taken to be more authoritative than a plain From. If a Resent-, Remailed-, or Redistributed- version of either a From or Sender field is given, it is taken to be more authoritative than the plain version of either. All such Re* headers are taken to be equally authoritative, and the last one seen in the header (the one furthest down in the header) is taken to be most authoritative. To determine if the user is who they claim to be, the local-address part of the most authoritative sender is looked up in the password file to map it to a UID, and that UID is compared to the invoking UID. If the UIDs match and the hostname part of the address is a name for the local system, the user is who they claim to be.
- A new parameter, **S**, indicates to use a Sender: field instead of a Source-Info: field, and also causes conflicting Sender: fields in the submitted header to be elided.
- Both lower and upper case characters are now used in queue file names and message-IDs. This allows up to 2704 messages to be queued by a single instance of submit. submit will refuse to accept further messages after that point. submit previously would use only lower case letters, and would use non-ASCII characters after those ran out.

Improvements to the local delivery channel: maildelivery(F)

The following changes have been made to **maildelivery**(F):

- Messages piped into processes via pipe aliases or the "Pipe" action in a user's *.maildelivery* file are now prefixed with a "From" header. This is important for various mail-processing applications, like **procmail**, **elm**'s **filter**, and **mailman**. Any workarounds (like **preline**) that add a pseudo-"From " line should be removed.
- Variables (like **$(address)**, **$(sender)**, and **$(reply-to)**) used in *.maildelivery* Pipe actions that expand to nothing are now replaced with an empty argument instead of being elided.

Improvements to the smtp channel

The following changes have been made to the smtp channel and are documented in the newly added **smtp**(ADM) and **smtpd**(ADM) manual pages:

- Interpretation of SMTP response codes is now compliant with RFC1123. All 5xx codes are taken to be indications of permanent failure. Failure codes in the initial greeting message and in the response to a HELO are recognized.
- The port number given for **smtp** in */etc/services* will be used. The default is 25.
- Two new timing parameters control the behavior of the smtp channel when connecting to a remote SMTP server to deliver an outbound message:

  open_timeout

  220_timeout

  See the **smtp**(ADM) manual page for more information.

- Per RFC2505, the SMTP channel can be configured to reject messages with a return address (envelope sender) that contains a domain name that does not resolve in a manner that would allow mail to be sent to it, meaning that the message could not be bounced if necessary. This is done with the **vrfy_sender_domain confstr parameter**.
- A colon-separated list of hostnames/addresses that should be treated as though they do not actually exist can be given with the **no_such_domain_hosts confstr** parameter. This is used in conjunction with the **vrfy_sender_domain** parameter. See the new **smtpd**(ADM) manual page for more information.

Improvements to the badusers channel

The **badusers** channel is intended to map usernames on the local host to the same usernames on a different host. It intentionally strips the hostname from the recipient address when it does this mapping so that the destination host will treat the recipients as local users. However, it is now common for mail systems to be configured to refuse to accept a recipient address that contains only a user name. If the badusers channel is used to forward mail to a host that is not under the control of the same administrator (for example, a host that is doing virtual mail hosting), this may present a problem. To resolve this, the badusers channel has two new confstr parameters, keepdomain and defdomain. Refer to **submit**(ADM) for more information.

Improvements to the uucp channel: rmail(ADM)

rmail(ADM) is now executable by group *uucp*, and not other, to prevent the authority of the UUCP system to inject messages with any sender name from being used by local users. It is possible that some extremely old software expects to be able to use rmail to inject messages locally. If this is the case, change the mode of **/usr/bin/rmail** to allow others to execute it:

chmod o+x /usr/bin/rmail

Improvements to cleanque(ADM)

cleanque(ADM) no longer sends warnings about messages that were queued with the no-return flag. **cleanque** also has a new command line option (**-t**) that displays the actions it would take on queued messages without actually doing anything.

CUPS printer subsystem

This feature was originally provided in the Update Packs and then Maintenance Pack 4.

The Common UNIX Printing System (CUPS) is unchanged in Maintenance Pack 5 (1.1.23). When installed, both the CUPS and standard (SYSV) print systems are active. Although both systems use the same command names, the options and behavior differ somewhat (each print system has a separate set of commands stored in */usr/lib/lp/cups* and */usr/lib/lp/sysv*):

accept cancel disable enable lp lpadmin lpmove lpr lpstat reject

Both command sets are supported. To make it easier to use the commands, you can define the default command set (SYSV or CUPS) to be used when a print command (such as **lpstat**) is entered on the command line. This can be done in any of three ways:

- on a system-wide basis in */etc/default/lpd*. The default entry is for the SYSV print system:
  PRINT_SYSTEM=SYSV
- on a per-login basis by including **PRINT_SYSTEM=CUPS** or **PRINT_SYSTEM=SYSV** in the environment.
- by including **--sysv** or **--cups** as the first argument in the print command line (example: **lpstat --sysv -t**).

When the pathname is not supplied, the commands from the default print system are executed. You can use the full pathname to run a command belonging to the non-default print system. In a similar way, you can access the manual pages for the two printer systems by supplying the relevant section name in the **man**(C) command (1 or 8 for CUPS man pages, C or ADM for the SYSV man pages):

Command	CUPS	SYSV
accept	8	ADM
cancel	1	C
disable	8	C
enable	8	C

lp	1	C
lpadmin	8	ADM
lpmove	8	ADM
lpr	1	C
lpstat	1	C
reject	8	ADM

The CUPS package installs the following online documentation -- the *Overview of the Common UNIX Printing System*, *CUPS User's Manual*, *Software Administrator's Manual*, and *CUPS Security Report*.

CUPS Administration

The CUPS distribution includes a web-based administrative interface that is configured on port 631 (*http://localhost:631*).

NOTE: You may have trouble logging in as *root* to the CUPS web administrative interface if each of the following three conditions are true:

1. Your system was installed with a Traditional or Low security profile.
2. You set a root password longer than eight characters during installation.
3. The *root* password has not been changed since installation.

In this case, use the **passwd**(C) command to re-enter the existing *root* password or change the password to a different value.

A list of available printers is generated at the time the CUPS print daemon (**cupsd**) is started (when the system enters multiuser mode). To regenerate the list (such as after connecting a new USB printer), enter the command:

/etc/init.d/cups restart

NOTE: Do not change the configuration for a printer (such as dpi) while it is printing. This has been known to corrupt the output of the print job.

CUPS and Remote Printing (LPD)

Although CUPS supports LPD as both a server and a client, the CUPS LPD server implementation does not support access control (based on the settings in the

/etc/hosts.equiv and */etc/hosts.lpd* files). If your setup requires the use of the standard LPD, or you wish to use access control, do not install CUPS.

WARNING: If you have never run **mkdev rlp** and you wish to do so, the CUPS package must be removed before running **mkdev rlp** and then reinstalled after remote printing is configured.

Using CUPS as an LPD client

To configure CUPS so that jobs can be sent to a remote LPD printer, add a printer via the CUPS administrative interface and use the following settings:

Attribute	**Setting**
Device	LPD/LPR Host or Printer
Prototype device URI	lpd://***hostname*/*printername***
Model/driver	Raw

NOTE: If the printer was already configured for remote printing, the host and printer name are present in the */etc/printcap* file.

Using CUPS as an LPD server

To configure CUPS so that remote hosts can send jobs to the CUPS printing system on the local host using the LPD protocol, follow the instructions found in the ``Printing to LPD Servers'' section of the *Software Administrator's Manual* in the online CUPS documentation.

WARNING: Because only one service can listen for print requests on the LPD port, **mkdev rlp** must not be configured on the local host. If **mkdev rlp** has ever been run on the host, it must be run again either before CUPS (MP4) is installed or with CUPS temporarily removed as described previously. If you intend to use CUPS as an LPD server you should run **mkdev rlp** to de-configure remote printing before CUPS/MP4 is installed (this is because the CUPS configuration is lost when the package is removed).

CUPS lpstat(1) command

The CUPS **lpstat**(1) always reports the state of devices as having been last modified on January 1st at 00:00. For example:

```
Obie accepting requests since Jan 01 00:00
```

This is because the CUPS version of **lpstat** does not capture this information. The default date is generated so that applications that parse **lpstat** output will not fail.

CUPS and HP LaserJet 6 Printers (PCL)

There is a known problem with the default printer driver displayed in the CUPS administrative interface for the HP LaserJet Series PCL 6. You should instead select one of these drivers that are reported to work:

- HP LaserJet Series CUPS v1.1 (en)
- HP LaserJet 6 series, CUPS+Gimp-Printv4.2.5 (en)

GIMP-Print support

This feature was originally provided in the Update Packs and then Maintenance Pack 4.

Maintenance Pack 5 provides the GIMP-Print (4.2.5) printer drivers for use exclusively with the CUPS printing system. GIMP-Print rasterizes bit images for printers that do not have built-in rasterizers (including many of the more inexpensive USB printers on the market).

The GIMP-Print package installs the following online documentation -- the *GIMP-Print User's Guide* and *GIMP-Print, The Print Plugin for the GIMP*.

ESP Ghostscript

This feature was originally provided in the Update Packs and then Maintenance Pack 4.

Maintenance Pack 5 includes the 8.15.1 release of ESP Ghostscript. This is installed by default in conjunction with GIMP-Print to provide better printer support with CUPS.

Foomatic printer drivers

This feature was originally provided in the Update Packs and then Maintenance Pack 4.

The foomatic package contains a generic printer filter and PPD (PostScript Printer Definition) files for over 200 non-PostScript printers. The filter and PPD files are integrated with the CUPS package and cannot be used with the System V LP print system. (Note that the CUPS package also provides its own PPD files. For more information, see the Printing topic in the online documentation.)

Further documentation on the printers supported by foomatic is available at:

http://www.linuxprinting.org/printer_list.cgi

You can search this site for the proper driver name for your printer, then look for the driver in the Make/Model selection list displayed by the CUPS graphical interface.

Foomatic is also a standalone system that creates PPD files from an XML database and includes tools for direct printing. The PPD creation program is called **foomatic-rip**(1) and the database is called *foomatic-db*.

Note that the Foomatic package provides the following manual pages:

foomatic-configure(1)
foomatic-gswrapper(1)
foomatic-ppd-options(1)
foomatic-ppdfile(1)
foomatic-printjob(1)
foomatic-rip(1)
foomatic-perl-data(1)
foomatic-compiledb(1)
foomatic-combo-xml(1)
foomatic-kitload(8)
foomatic-preferred-driver(8)
foomatic-getpjloptions(8)
foomatic-addpjloptions(8)

Extended shells

This feature was originally provided in the Update Packs and then Maintenance Pack 4.

The latest, stable versions of the GNU Bourne-Again Shell (**bash**), Z-Shell (**zsh**), and Extended C-Shell (**tcsh**) are provided in Maintenance Pack 5. Documentation for each of the shells, including manual pages and texinfo help, is provided when the shells are installed.

GNU Bourne-Again Shell (**bash**) version 3.1.1

> This popular shell from the GNU Project is a feature-rich shell that is largely IEEE POSIX P1003.2 compliant. It has most features of the Korn Shell (**ksh**) and is well suited to interactive use. Most existing shell scripts should run correctly with **bash**.

Z-Shell (**zsh**) version 4.2.6

> This shell is best suited for interactive usage. It has highly programmable command and filename completion, is most compatible with the Korn Shell (**ksh**), and has features that C-shell (**csh**) users will find familiar. It also has a full FTP client that you can access with built-in shell commands, as well as a number of additional loadable modules. You can extend **zsh** with other third-party modules at any time.

Extended C-Shell (**tcsh**) version 6.14

This is a Berkeley C-shell (**csh**) compatible shell with many improvements, bug fixes, and command line editing capabilities. Note that the SCO version of **csh** behaves differently from other implementations of **csh** (including **tcsh**) in implementation of the || and **&&** operators.

Korn Shell 93r (**ksh**)

This is the latest revision of the original Korn Shell, which adds a number of new (mostly scripting-related) features, including lexical scoping, compound variables, associative arrays, named references and floating point math. In addition, "tab-style" command and filename completion is supported and the use of cursor keys to navigate the shell history works much better than in ksh88.

Vim text editor

Maintenance Pack 5 now includes **Vim**, version 7.0.0. **Vim** is a highly configurable text editor that is intended to increase text editing efficiency. It is an improved version of the **vi**(C) editor.

See the **vim**(1) manual page for more information.

Updates to UDK compatibility libraries

First provided in Maintenance Pack 3.

Maintenance Pack 5 includes version 8.0.2b of the UDK compatibility libraries, which contains several fixes to the runtime libraries, including:

- fixed bad parsing of some special strings in string-to-floating code
- corrected a potential infinite loop in **thr_create**()
- fixed a memory leak in **tzset**()

Fixes provided in the Maintenance Pack

Maintenance Pack 5 includes the following fixes:

Commands and Utilities

1. **apc portcheck utility uses poor test for whether port is a modem-control device** --
   The APC UPS daemon setup procedure now works properly with any serial port that implements wait-for-DCD open() behavior.
   (ID: 533261:2)
2. **acctcom enhancements** --
   acctcom has several new options. For a summary do "acctcom -X".
   (ID: 533850:1)
3. **calendar program treats itself as a calendar** --
   calendar no longer checks for whether pseudo-users have calendar files. This corrects a problem with erroneous calendar messages being mailed to sysinfo on certain days of the year.
   (ID: 533589:1)
4. **Misassigned video card memory address for VMware (caused X server restarts to fail)** --
   This problem has been resolved.
   (ID: 533852:1)

Development System

5. **Extended DST requires new timezone rules** --
   The US Daylight Saving Time rules were changed in 2005 to come into effect in 2007. DST starts at 2am (local time) on the second Sunday of March, and ends at 2am on the first Sunday of November.
   (ID: 532758:5)
6. **Update mcs to generate correct binaries** --
   This problem has been resolved.
   (ID: 533854:1)
7. **Miscellanous memory leaks in Motif** --
   Memory is no longer leaked when shell widgets are created and destroyed.
   (ID: 533105:2 ESC: erg712964)
8. **UW7 libc strtod() patch** --
   A UW7 patch to strtod() was applied (needed for pgsql).
   (ID: 533857:1)

Kernel

9. **STREAMS ioctls conflict with console ioctls for OSR binaries** --
   A STREAMS I_PEEK on a console tty device will no longer switch the console to a graphic mode.
   (ID: 533690:2)

Installation

10. **sco_pmd: Prevent DOS attack on CPD port if incomplete packets are received** --
    This problem has been resolved.
    (ID: 533860:14)
11. **OSR 5.0.7 MP removal does not restore prior sys5.o object file** --
    Fix for MP5 prior (MP3/MP4) install bug where removal of the MP did not restore the previous sys5.o object file to the /etc/conf/pack.d/os.a archive.
    (ID: 533953:1)

Networking

12. **POP daemon garbles mail on server** --
    popper no longer corrupts mailboxes.
    (ID: 532730:2)
13. **New traceroute options added** --
    Added -f (first-ttl) and -Q (max-timeout) options to traceroute.
    (ID: 533858:1)

Operating System

14. **Remove sconf test for whether invoking user is root** --
    sconf can now be run by ordinary users. It will only succeed if the invoking user has read/write access to /dev/scsi.
    (ID: 533851:1)
15. **kmem_alloc panic in scloaduser from mapkey** --
    Fixed a bug that caused occasional kernel panics when executing the mapkey command.
    (ID: 533418:2)
16. **Improvements to getty** --
    Fixed a problem with getty that did not allow a serial port to be used for dialout.
    (ID: 533149:4)

Security

17. **Xloadimage NIFF Image Title Handling Buffer Overflow** --
    This problem has been fixed.
    (ID: 533253:5)
18. **Lynx Remote Buffer Overflow** --
    Lynx 2.8.5rel.5 resolves remote exploitation of a command injection vulnerability.
    (ID: 533314:5)
19. **Apache 1 CRL Issue** --
    Fixed an off-by-one error in the mod_ssl Certificate Revocation List (CRL) verification callback in Apache that could be exploited to cause a buffer overflow.
    (ID: 532917:2 ESC: erg712919)

20. **Apache mod_imap "referer" cross-site scripting vulnerability** --
    Cross-site scripting (XSS) vulnerability was resolved in the mod_imap module of Apache httpd.
    (ID: 533444:5)
21. **CUPS xpdf Buffer Overflow Vulnerabilities** --
    Mulitple overflow vulnerabilities in CUPS were addressed by patch to xpdf.
    (ID: 533446:4)
22. **ICMP TCP connection vulnerability** --
    Corrected a vulnerability where TCP connections could be degraded or dropped.
    (ID: 530662:2 ESC: erg712759)
23. **Vulnerability issues in TCP; NISCC Vulnerability Advisory 236929** --
    A denial of service vulnerability in TCP has been addressed.
    (ID: 529385:1 ESC: erg712599)
24. **Bind 8.4.6-REL released fixes several security issues** --
    (ID: 531004:2 ESC: erg712788)
25. **libXPM vulnerability** --
    Corrected a vulnerability that could allow attackers to execute arbitrary code.
    (ID: 533161:3)
26. **xpdf buffer overflow vulnerabilities** --
    [SCOSA-2006.15] xpdf has been updated to version 3.01pl2 to address several problems.
    (ID: 533384:3)
27. **ESP Ghostscript 7.x vulnerability** --
    Insecure temporary file creation vulnerability addressed by update to ESP Ghostscript 8.15.1.
    (ID: 533156:4)
28. **gdk-pixbuf/gtk+ XPM buffer overflow** --
    Fixed vulnerability in GTK+ gdk-pixbuf XPM image rendering library.
    (ID: 533256:5)
29. **OpenSSL SSL 2.0 Rollback** --
    OpenSSL has been updated to 0.9.7i/0.9.6m to address a vulnerability affecting applications that use the SSL/TLS server implementation.
    (ID: 533160:5)
30. **Mozilla multiple vulnerabilities** --
    Mozilla has been updated to version 1.7.13.
    (ID: 533769:3)
31. **Java security issues** --
    Java has been updated to fix several vulnerabilities.
    (ID: 532204:2 ESC: erg712841)
32. **Mozilla Suite History Information Denial of Service** --
    Mozilla has been updated to version 1.7.13 to address this vulnerability.
    (ID: 533443:4)
33. **Perl format string integer wrap vulnerability** --
    Perl has been updated to fix an integer overflow in the format string functionality.
    (ID: 533382:4)

34. **php Trailing Slash "open_basedir" Security Bypass** --
    PHP has been updated to version 4.4.2 to address this issue.
    (ID: 533152:4)
35. **php <= 4.4.0 multiple vulnerabilities** --
    PHP has been updated to version 4.4.2 to address several vulnerabilities.
    (ID: 533301:4)
36. **php < 4.4.1 htaccess apache DoS** --
    PHP has been updated to version 4.4.2 to address this issue.
    (ID: 533378:4)
37. **php < 4.4.1 denial of service vulnerability** --
    PHP has been updated to version 4.4.2 to address this issue.
    (ID: 533379:4)
38. **php "mb_send_mail()" "To:" header injection vulnerability** --
    PHP has been updated to version 4.4.2 to address this issue.
    (ID: 533381:4)

    Other Fixes

39. **Java security problems** --
    Unannounced security fixes resolved in J2SE 1.4.2.11.
    (ID: f533660:1)
40. **Java font problems** --
    Fonts on UnixWare and OpenServer that appeared "fuzzy" have been swapped with Sun-provided TrueType fonts.
    (ID: 533374:1)
41. **Java plugin vulnerabilities** --
    Multiple vulnerabilities in Java plugin addressed in 1.4.2_09.
    (ID: 533319:1)
42. **Java timezone fixes** --
    Timezone changes/updates 1.4.2.11 and 1.4.2.12.
    (ID: 533661:1, 533833:1)
43. **Java: fsync() issued on input file results in hotspot failure** --
    This issue has been resolved.
    (ID: 533606:1)

Fixes provided in previous Maintenance Packs

SCO OpenServer Release 5.0.7 Maintenance Pack 4 included the following bug fixes:

- Fixed a problem where the **Network Client Manager** was getting a fatal error when used by any user other than *root*.
  fz533088
- The DocView URL rewriting rules now handle filenames like *.*html.*<***language***> correctly.
  fz529697

- Fixed a problem which first occurred in the 2.0.0Eb version of GWXLIBS that made Mozilla interpret the "q" key as a tab.
  fz533010
- SCO OpenServer Release 5.0.7 MP3 broke */etc/lmcfsd*. It has now been fixed.
  fz530299 / erg712716
- Clicking on the "?" on the lower toolbar no longer crashes **xpdf**.
  fz532798
- In the SCOadmin **DHCP** Server Manager in CHARM mode, **Entry** -> **Add** -> **Address Pools** was resulting in a hang. This is now fixed.
  fz532170
- **/usr/sbin/menu** no longer dumps core with a simple menu screen.
  fz532986
- Parallel printer polling mode now works.
  fz532780 / erg712891
- In CHARM mode it is now possible to add hosts to the */etc/host* file using the SCOadmin **Network Client Manager**.
  fz530820
- Enabling kprf (kernel profiling) on an SMP system was causing a panic. This has been fixed.
  fz528869 / erg712549
- Fixed a problem where the **audit** daemon was creating files with permissions set to 000.
  fz531480 / erg712842
- A timing race which could cause **telnet**/**rlogin** output to hang on an SMP system was found and fixed.
  fz525805
- **iknt** was fixed so that **rlogin** now works when **iknt** is disabled.
  fz525874
- General cleanup was done on the **relax**(ADM) scripts.
  fz529525
- **cron** was fixed so that jobs will not fail when the */etc/default/login* **ULIMIT** is higher than the kernel default.
  fz530027
- **ndc**(ADMN) was getting a `Socket is not connected` error on SMP systems. This was fixed in the socket driver.
  fz527413
- A fix was made to **telnetd** for an intermittent character loss problem.
  fz530296
- The spacing between the IP address and the host name was improved in the **Network Client Manager** in CHARM mode.
  fz530970
- Handling of multiple NICs was improved in the DHCP Client.
  fz531650
- Fixed a problem where the SCOadmin **Network Client Manager** was not saving the domain search order settings.
  fz532183

- Fixed a problem where the SCOadmin **Network Client Manager** was not handling the pound sign start-of-comment character in *ntp.conf*.
  fz532302
- The extended shells have been added to the **Account Manager** shell selection options.
  fz528748
- An escape sequence for changing the color of text displayed on the console was not working; this has been fixed.
  fz530387 / erg712723
- **bash** was fixed to process the *.inputrc* file.
  fz531964
- Running the **setclk -v** command twice in a row would cause the RTC to jump by the delta from UTC if the */etc/rtc.data* file existed. Fixed.
  fz530715 / erg712764
- In the **Network Client Manager**, the display of the ``Comments'' field in the */etc/hosts* option was improved.
  fz531269
- The SCSI configuration viewing utility (**/usr/bin/rview**) provided with the Tricord ES5000 (**iiop**) HBA driver has been changed to **/usr/bin/iiop_rview** to prevent a conflict with an export from the **Vim** package. The **iiop**(HW) manual page has been updated with the new utility.
  fz532889
- **dfspace**(C) was fixed to show information for all mounted filesystems.
  fz530011
- Various programs which use sockets in non-blocking mode, such as ndc and Postfix, would cause these kernel messages to appear on SMP systems:

```
WARNING: soreceive: unexpected message type x00000083
WARNING: soreceive: not M_DATA, found 131
```

  This was fixed in the socket driver.
  fz529156 / fz532437 / erg712795

- The **a15k** driver was fixed to not interfere with the **ad320** adapter.
  fz529926
- Fixes were made for the Dell GX280.
  fz530306
- USB devices attached to an EHCI controller sometimes would get a message logged to the console, `Device reset timeout during enumeration!`, even though the USB driver would automatically recover from the timeout. The driver was fixed to eliminate the unnecessary message.
  fz530377
- A timing race between the **fork**() system call and the **ps**(C) command was found and fixed. It would sometimes cause a newly forked child process to hang in **genfork**().
  fz532293 / erg712846

- Fixed a memory leak which would occur when opening a message catalog if the catalog did not start with message number 1.
  fz529104 / erg712578
- A fix was made so that the X server display will not be corrupted when data is written to **/dev/console** when NSCRN=1 and an ATI video card is used.
  fz529459 / erg712612
- The latest processor errata microcode drop from Intel is included.
  fz529620
- A fix was made to the X server function cfbPolyFillRect() to prevent a core dump.
  fz530567 / erg712742
- A buffer overflow in **zip** has been fixed.
  fz530928 / CAN-2004-1010
- A cross-site scripting flaw in **htsearch** which affected DocView was fixed.
  fz531484 / CAN-2005-0085
- A fix was made to the **ip** driver for the ``Rose Attack'' vulnerability.
  fz529415 / CAN-2004-0230 / SCOSA-2005.9
- A vulnerability in **cscope** was fixed.
  fz530504 / CAN-2004-0996 / SCOSA-2005.11
- A command line buffer overflow in **/usr/lib/sysadm/termsh**, **atcronsh**, and **auditsh** was fixed.
  fz527464 / CAN-2005-0351 / SCOSA-2005.15
- A bug which allowed a chroot prison to be broken was fixed.
  fz528523 / CAN-2004-1124 / SCOSA-2005.22
- Two vulnerabilities were fixed in the **telnet** client.
  fz531456 / CAN-2005-0469 / CAN-2005-0468 / SCOSA-2005.23
- Multiple vulnerabilities were fixed in **libpng**.
  fz530148 / CAN-2004-0597 / CAN-2004-0598 / CAN-2004-0599 / SCOSA-2005.30
- A vulnerability was fixed in **zlib**.
  fz530157 / CAN-2004-0797 / SCOSA-2005.30
- Multiple vulnerabilities were fixed in **libtiff**.
  fz531016 / CAN-2004-0803 / CAN-2004-0804 / CAN-2004-0886 / CAN-2004-0929 / CAN-2004-1183 / CAN-2004-1308 / SCOSA-2005.30
- Multiple vulnerabilities were fixed in **bzip2**.
  fz532328 / CAN-2005-0953 / CAN-2005-1260 / SCOSA-2005.30
- A **telnet** client vulnerability was fixed.
  fz532339 / CAN-2005-0488 / SCOSA-2005.35
- A vulnerability in **unzip** was fixed.
  fz532853 / CAN-2005-2475 / SCOSA-2005.39
- A vulnerability in OpenSSH related to SCP client file corruption was fixed.
  fz529677 / CAN-2004-0175
- Multiple vulnerabilities were fixed in PHP.
  fz529882 / CAN-2004-0594 / CAN-2004-0595

- Multiple vulnerabilities were fixed in PHP.
  fz530691 / CAN-2004-1018 / CAN-2004-1019 / CAN-2004-1063 / CAN-2004-1064
- Multiple vulnerabilities were fixed in PHP related to the exif and fbsql extensions as well as the unserialize(), swf_definepoly() and getimagesize() functions.
  fz532342 / CAN-2005-0524 / CAN-2005-0525 / CAN-2005-1042 / CAN-2005-1043
- Multiple vulnerabilities were fixed in Perl.
  fz531488 / CAN-2004-0452 / CAN-2004-0976 / CAN-2005-0155 / CAN-2005-0156 / CAN-2005-0077
- A buffer overflow in **libtiff** was fixed.
  fz532776 / CAN-2005-1544
- Buffer overflows in **zlib** were fixed.
  fz532828 / CAN-2005-1849 / CAN-2005-2096 / CAN-2004-0797
- Multiple security issues were fixed in **gzip**.
  fz532855 / CAN-2005-0758 / CAN-2005-0988 / CAN-2005-1228
- A vulnerability was fixed in CUPS.
  fz530152 / CAN-2004-0558
- A **wu-ftp** denial of service issue was fixed.
  fz532335 / CAN-2005-0256
- A vulnerability was fixed in **cdrecord**.
  fz530155 / CAN-2004-0806
- Several security vulnerabilities in Squid were fixed.
  fz530962 / SQUID-2004:3 / SQUID-2005:1 / SQUID-2005:2 / SQUID-2005:3
- Denial-of-Service issues found in Squid 2.5.STABLE10 and earlier were fixed.
  fz533116 / fz533151 / CAN-2005-2794 / CAN-2005-2796 / CAN-2005-2917
- A Denial-of-Service issue found in Squid 2.5.STABLE11 and earlier was fixed.
  fz533254 / CVE-2005-3258

Maintenance Pack 3 included the following bug fixes:

- **fdisk**(ADM) no longer writes the partition table with the kernel cached copy when just viewing the table.
  fz529555
- Fixed a security vulnerability caused by a misconfiguration of the Apache server that allowed remote users to view any publicly readable file.
  fz528125/erg712368/CAN-2003-0658/CSSA-2003-SCO.16
- A series of vulnerabilities in the SSL/TLS library that could allow DOS attacks were addressed in OpenSSL 0.9.7d.
  fz529412/CAN-2004-0079/CAN-2004-0112/CAN-2004-0081
- Fixed a problem where the **ct** utility failed to display a login prompt after dialback.
  fz300580
- **uucpd**(ADMN) now accepts other paths for **uucico** and now logs login successes/failures via **syslog**.
  fz529101

- **uucico**(ADM) no longer dumps core on large files when using **t** protocol over satellite connection.
  fz527175
- When creating a filesystem name longer than 7 characters in **divvy**(ADM) during install or after install, all the letters after the 7th would appear in the FS TYPE column. This has been fixed.
  fz528538
- The **netconfig** "Add new LAN adapter" option no longer displays LAN cards that are already configured.
  fz527523/erg712306
- Fixed problem where **Xsco** failed to start properly with non-C locales with certain graphics chips.
  fz528991
- Support for the X authorization protocols has been added for X sessions that are not started by scologin.
  fz520452/erg712002/CAN-2004-0390/SCOSA-2004.5
- **smtpsrvr** de-referenced a null pointer and core dumped in response to certain DNS failures when attempting to resolve the source hostnames. This has been fixed.
  fz527610
- The **shutdown**(ADM) utility once again displays times in a meaningful format.
  fz529090
- **mailx**(C) would hang if execmail died unexpectedly. This has been fixed.
  fz529102
- A fix was made to prevent a potential panic in **getsockopt()**.
  fz528029
- **setcontext()** now restores the EDX register correctly.
  fz528232
- A buffer overflow with the **Xsco -co** option has been fixed.
  fz520528/erg712006/CAN-2002-0155/CSSA-2003-SCO.26
- **uudecode**(C) now checks if the specified output is a symlink or pipe.
  fz527541/erg712054
- A panic lock timeout from vdsendbuf+53 during vdisk repair was fixed.
  fz527937/erg712320
- Several buffer overflows were fixed in the processing of the *font.alias* files in **Xsco**(X).
  fz528866/erg712547
- A problem where the X server would allow access to any shared memory on the system has been fixed.
  fz520242 / erg711972 / CAN-2002-0164 / CSSA-2003-SCO.26
- A problem in the SCO **Internet Manager** (mana) that let local users gain *root* level privileges was fixed.
  fz528244 / erg712420 / CAN-2003-0742 / CSSA-2003-SCO.19
- Multiple buffer handling problems were fixed in OpenSSH.
  fz528324 / erg712436 / CAN-2003-0693 / CAN-2003-0786 / CAN-2003-0695 / CAN-2003-0682 / CSSA-2003-SCO.24

- A number of security issues were fixed in Apache.
  fz527514 / erg712258 / fz528422 / erg712464 / fz528484 / erg712486 / fz528487 / erg712489 / fz527929 / erg712354 / CAN-2003-0192 / CAN-2003-0542 / CAN-2002-1396 / CAN-2003-0166 / CAN-2003-0442 / CSSA-2003-SCO.28
- Several security issues were fixed in the OpenSSL and **zlib** components of **gwxlibs**.
  fz528382 / erg712448 / fz527506 / erg712256 / fz527489 / erg712252 / CAN-2003-0543 / CAN-2003-0544 / CAN-2003-0545 / CAN-2003-0131 / CAN-2003-0107 / CSSA-2003-SCO.29
- A cross-site scripting vulnerability in the **CGI.pm** perl module was fixed.
  fz528215 / erg712409 / CAN-2003-0615 / CSSA-2003-SCO.30
- Various buffer overflows and other security issues were fixed in MMDF.
  fz528322 / erg712434 / SCOSA-2004.7
- **pmwm** and **mwm**(XC) were fixed to allow the key binding for <Ctrl>-<Alt>-<Shift>-1 to be changed or disabled.
  fz528631 / erg712515
- A system hang was fixed. It was caused by **strd** looping and trying to allocate memory for message headers when the mblock table was full. fz527661 / erg712281
- A number of security issues were fixed in Mozilla.
  fz528708 / erg712531 / SCOSA-2004.8
- **getty**(M) now includes a **-r** option that prevents it from dropping DTR and resetting the termio modes at startup. This was the default behavior in OpenServer 5.0.6 but it was changed in OSR5.0.6a. The **-r** option can be used to revert to the OpenServer 5.0.6 behavior. Some third-party applications wait for incoming calls, initialize the termio parameters, and then invoke getty to initiate a login session. In this case, to avoid dropping connections when getty is invoked, the **-r** option should be used by editing both */etc/inittab* and the appropriate file under */etc/conf/init.d* (for standard serial ports, this would be */etc/conf/init.d/sio*) and adding the **-r** option to the **getty** lines that should have their behavior modified.
  fz527207 / erg712222

Maintenance Pack 1 included the following bug fixes:

- A remotely exploitable off-by-one bug was fixed in the wu-ftp FTP sender.
  fz528115 / erg712363 / CAN-2003-0466 / CSSA-2003-SCO.20
- A problem that prevented kernel builds from succeeding if **$ROOT** was longer than 60 characters has been fixed.
- The licensing system has been corrected so that the **brand**(ADM) command now recognizes pre-Release 5.0.7 User and CPU licenses. In addition, the Licensing Policy Manager Daemon (**sco_pmd**) has been fixed so that system restores now correctly restore the SCO System ID. This fix makes the OSS646 supplement obsolete and unnecessary.
  fz527794
- A panic was corrected in the HTFS filesystem driver. This panic sometimes occurred when mounting an AFS, EAFS, or HTFS filesystem with less than

42Kbytes of free space.
fz527790

- A problem on USB keyboards where typed characters sometimes repeated has been fixed.
  fz527743
- Fixed a null dereferencing problem in MMDF.
  fz527660
- Changed MMDF format specs so that the date registered in email headers is padded with a leading zero if the message is sent in a single-digit hour (between 1:00 and 9:00). This addresses the problem of some anti-spam applications assigning high spam scores to messages simply because the format of the hour in the date header does not match the applications' good-date-header test, which expects hours to be represented in double-digits.
- Fixed a security vulnerability in the **sendmail** binary that could be exploited by remote users to gain *root* access.
  fz527482/erg712245/CSAA-2003-SCO.6
- The **chmod**(C) command was modified so it does not apply changes to files if permissions are already correct. This modification may significantly improve performance, especially over an NFS mount, of commands like:
  chmod -R +r /data
- The **crontab**(C) command has been corrected to always exit with an error status if it fails, or zero (no error) status if it succeeds.
  fz300043
- Fixed the **ps**(C) command so the **-o pcpu** option reports an accurate value.
  fz527713
- A problem was corrected which caused **uudecode**(C) to dump core when decoding from standard input.
  fz527731
- A buffer overflow in the **wordwrap**() function in releases of PHP previous to version 4.3.0 and later than version 4.1.2 has been fixed. Under certain circumstances, this buffer overflow created a security vulnerability.
  fz527514 / erg712258
- Fixed a security vulnerability where a TCP/IP socket could become permanently stuck in a SYN_SENT state, thereby making the system vulnerable to a denial-of-service attack.
  fz526775 / erg712173 / erg711405
- The problem of data transfers not always working if the FTP daemon was configured in */etc/services* to run on a non-standard port or if the daemon was invoked with the **-P** argument has been fixed.
  fz527753
- The **telnetd**(ADMN) command now has a **-r** option to specify which pseudo-terminals (ptys) to use, which is useful in the following situations:
  - Restrict **telnetd** to using ptys in a given range, so that other ptys can be dedicated to other functions.
  - Assign a **telnetd** that is bound to a particular non-standard port a specific pty so that a login on that port will always get the same pty name (as

required by some older applications created when hard-wired serial terminals were the norm).

See **telnetd**(ADMN) for more information.
fz527717 / erg712178

- Integer overflow vulnerabilities were corrected in SUNRPC **adr_array**(), **xdrmem_getbytes**(), and related functions. Theoretically, these vulnerabilities could be exploited to gain a privilege escalation.
  fz525724 / fz526830 / erg501641 / erg712178 / CA-2002-25 / CAN-2002-0391 / CAN-2003-0020
- A buffer overflow in BIND that could lead to security vulnerabilities has been fixed.
  fz526617 / erg712158 / CSSA-2003-SCO.17 / CAN-2002-1219
- Fixed some minor problems in the **PPP Connection Wizard** interface.
- Fixed an SMP problem where PCI interrupt sharing was broken when one or more of the drivers sharing an interrupt was able to handle the interrupt on any processor. Symptoms of this problem included spurious and lost interrupts.
  fz526928
- Fixed a panic that occurred when booting a system with SMP installed. The panic occurred most commonly in **kmem_alloc**() while the **/etc/sysdump -qi /dev/swap -o /dev/swap** command was running in a different process. Typically, this problem was encountered on systems with large swap areas (around 2.5GB) and the **usb_ohci** driver enabled.
  fz527402
- Fixed a problem that caused the Mylex/BusLogic **blc** SCSI HBA driver to fail when booting with SMP installed. The error message produced in this situation was:
- `WARNING: apic - no BIOS information found for irq` ***IRQ_NUM***
- Fixed a number of bugs in SCO OpenServer Development System header files and tools.
  fz527564 / fz527644 / fz527678
- The C Compilation Subsystem (CCS) has been updated to be more strictly gABI compliant. This includes changes to the assemblers, link editors, and startup files to support the special **.init_array** and **.fini_array** sections in ELF programs that certain third-party C++ compilers use.
  fz527038 / fz527718
- Security vulnerabilities were fixed in BIND.
  fz528463 / erg712478 / VU#734644
- Security vulnerabilities were fixed in OpenSSL.
  fz529412 / erg712603 / CAN-2004-0079 / CAN-2004-0112 / CAN-2004-0081
- A security issue was fixed in Apache related to mod_digest.
  fz528952 / erg712565 / CAN-2003-0987

Maintenance Pack notes and limitations

The following notes and limitations apply to Maintenance Pack 5:

- A consequence of the new USB/serial driver is that long, descriptive device nodes are created that exceed the hardcoded ttyname limit of the tty/login subsystem (9 characters). The long device name describes the actual topology of the device (PCI bus, PCI device number, host controller interface, and so on).

  If you intend to use a USB modem or a serial terminal for connecting directly to your OpenServer system (not using ppp), you need to create an alias for the device node that allows the modem or terminal to be properly treated as a login device. Follow this procedure:

  1. Prior to attaching your device, enter the following command:

     ls /dev/tty*[aA]
  2. After attaching the device, enter the command again and note the new device name added to the system.
  3. Create a new file called */etc/default/usbalias* and create an entry of the following format:

     /dev/***node***.A=/dev/***name***A
     /dev/***node***.a=/dev/***name***a

     where ***node*** is the device name added to the system when you plugged in the new device, and ***name*** is an alias that you define yourself.

     Here is an example:

     ```
     /dev/tty.0300110.A=/dev/usbmdm1A
     /dev/tty.0300110.a=/dev/usbmdm1a
     ```

  4. After creating or editing */etc/default/usbalias*, you must notify the **giomap_noded** daemon by sending a SIGHUP signal:

     kill -HUP *pid*

     where ***pid*** is the process ID of the **giomap_noded** process. You can also find the process number and send the signal with a single command:

     kill -HUP `ps -ef |grep giomap_noded|grep -v grep |awk '{print $2}'`

  NOTE: If you later change the name of an alias, you must manually delete the old alias node in */dev*.

- A security fix was introduced in Maintenenace Pack 4 to prevent illegal escapes from a **chroot** prison (ID: 528523). If you did not install MP4 and you remove

MP5, the chroot_security=1 setting remains in the *kernel/space.c* file. However, this security fix is not in effect until you re-install MP4 or later.

- Issues associated with running SCO OpenServer Release 5.0.7 on a Dell OptiPlex GX280 desktop, including problems with using USB devices, have been addressed through a combination of fixes. These fixes are available from an updated SCO OpenServer Release 5.0.7 System CD-ROM and SCO OpenServer Maintenance Pack 5. The updated SCO OpenServer Release 5.0.7 System CD-ROM has been shipping since 4 October 2005 and is labeled with the following part number:

  ```
  7OSR01A05072
  ```

  To install SCO OpenServer Release 5.0.7 on a Dell OptiPlex GX280 desktop:

  1. Use the updated SCO OpenServer Release 5.0.7 System CD-ROM, with the part number **7OSR01A05072**.

     At the `Boot:` prompt, always use the **uhcireset** bootstring to avoid the possibility of the system hanging when a USB floppy drive is attached to the system.

     defbootstr uhcireset

  2. If the GX280 system contains an IDE controller, you should also use the most current **wd** BTLD.

     defbootstr link=wd uhcireset

     The most current **wd** driver is is available on the SCO OpenServer Release 5.0.7 Supplement CD Version 5, as well as the SCO OpenServer Release 5.0.7 Supplements web page.

  3. After the SCO OpenServer Release 5.0.7 installation is complete, install Maintenance Pack 5.

- On SCO OpenServer Release 5.0.7 Host systems where networking is only configured for loopback (or network configuration is deferred at installation), the Apache webserver fails to start. (DocView does start and appears to be running.)

  There are two workarounds for this problem:

  A. Comment out the following lines in */usr/lib/apache/httpd.conf*:

  ```
  LoadModule unique_id_module   libexec/mod_unique_id.so
  AddModule mod_unique_id.c
  ```

  B. Set the hostname to the loopback address in */etc/hosts*:

```
127.0.0.1       yourhostname
```

- After installing SCO OpenServer Release 5.0.7 Maintenance Pack 5, you may need to update a few configuration files that are part of the GIMP Toolkit (GTK+) and necessary for operation of Mozilla. Some of the path names in the default configuration changed as of Maintenance Pack 3, but the upgrade process does not modify these files automatically because you may have customized them for your own purposes.

  Each file has a default file in the same directory. For most sites, you can simply copy the new default file to the data file. If you have loaded extra objects into these data directories, you may need to run a special command to produce the correct configuration file. The files affected are:

  /etc/pango/pango.modules
  To regenerate this file if you have added extra modules, use the command **pango-querymodules** after the upgrade and redirect the output of that program to this file. If you have not added any Pango modules, simply execute:

  cp pango.modules.default pango.modules

  /etc/gtk-2.0/gtk.immodules
  Regenerate this file using the command **gtk-query-immodules-2.0**, or copy the default using the command:

  cp gtk.immodules.default gtk.immodules

  /etc/gtk-2.0/gdk-pixbuf.loaders
  Regenerate this file using the command **gdk-pixbuf-query-loaders**, or copy the default file using the command:

  cp gdk-pixbuf.loaders.default gdk-pixbuf.loaders

  /etc/pango/pango.aliases
  If you have made changes, you may need to examine the new default file to see if there are specific changes you want to merge into your configuration file; otherwise copy the default file using the command:

  cp pango.aliases.default pango.aliases

  /etc/pango/pangorc
  If you have made changes, you may need to examine the new default file to see if there are specific changes you want to merge into your configuration file; otherwise copy the default file using the command:

  cp pangorc.default pangorc

/etc/pango/pangox.aliases
If you have made changes, you may need to examine the new default file to see if there are specific changes you want to merge into your configuration file; otherwise copy the default file using the command:

cp pangox.aliases.default pangox.aliases

/usr/lib/php.ini
This file also has an updated default file named */usr/lib/php.ini-dist*. If you are not an SCO Update Service customer and you copy the updated file over the existing *php.ini* file, please note that PHP will fail to load unless you comment out the PostgreSQL module. This can be found on line 552 of the default file:

```
extension=libpgsql.so
```

To comment out this entry, simply insert a semicolon (;) at the beginning of the line.

- Previously, the icons in */usr/lib/apache/icons* did not display in Apache because the icon directory and files are symbolic links. This also prevented test scripts located in */usr/lib/apache/cgi-bin* from running properly. To correct these problems, the **FollowSymLinks** option has been added to the */usr/lib/apache/conf/httpd.conf.default* file. If no modifications were made to the original file, you can copy the default file to */usr/lib/apache/conf/httpd.conf*. If you have customized the *httpd.conf* file, you must incorporate the change manually, as shown here:

```
<Directory "/usr/lib/apache/icons">
Options Indexes FollowSymLinks MultiViews
AllowOverride None
Order allow,deny
Allow from all
</Directory>
<Directory "/usr/lib/apache/cgi-bin">
AllowOverride None
Options FollowSymLinks
Order allow,deny
Allow from all
</Directory>
```

- If you did not install MP1 and you completed a backup of your system prior to installing Maintenance Pack 5, you should refresh the backup after you complete the installation of Maintenance Pack 5.

  If you need to restore a system using a backup that was created prior to the installation of Maintenance Packs 1, 3, or OSS656B, the Licensing Policy Manager Daemon (**sco_pmd**) may not start. If you experience this, log in as *root*, put the system in single-user mode, and run the following:

  brand -B oyrarg

Afterwards, reboot your system; the **sco_pmd** daemon will now be able to start.

- If you encounter a situation where you need to stop the Licensing Policy Manager Daemon (**sco_pmd**) -- for example, you are migrating a system on the network to new hardware and you start receiving duplicate license violations -- be sure to use the following command for an orderly shutdown:

  sco_pmd -s

  For more information on **sco_pmd**, including how to start and stop the daemon, see the **sco_pmd**(ADM) manual page.

- Several tunable parameters for the System V Inter Process Communications (IPC) shared memory and semaphore facilities were updated in MP2. The default settings were raised to values which should accommodate most commercial and open source databases without additional tuning. The maximum values of several parameters were also raised. The changes increase kernel memory usage by approximately 33K.

  As of MP2, installation of this Maintenance Pack raises the default and maximum values of these parameters as follows:

Parameter name	**Previous default**	**Previous maximum**	**New default**	**New maximum**
SEMMAP	10	-	256	-
SEMMNI	10	-	384	-
SEMMNS	60	-	512	-
SEMMNU	30	100	150	8192
SEMMSL	25	-	50	-
SEMOPM	-	10	-	1024
SEMUME	-	10	-	25
SHMMAX	524288	-	10485760	-
SHMMNI	100	-	200	-

  Individual parameters that have already been set higher than these values are not changed.

- At this time, Arabic and Georgian characters do not display correctly in the Mozilla web browser.
- If you are viewing the CUPS web-based administration tool (available from **http://localhost:631**) in the Mozilla web browser, there is a problem that prevents you from adding a printer using the **Printers** menu in the ESP bar.

Instead, use the **Do Administration Tasks** link on the main page of the CUPS administration tool. Then click the **Add Printer** button in the Printers category. See the online CUPS documentation, available from DocView, for more details on adding printers.

- Printing to an Epson Stylus C82 printer with CUPS and GIMP-print results in disjointed print-outs and many blank pages. A fix for this problem will be available in a future release.