UnixWare 7.1.4
Maintenance Pack 3
Release Notes

Dear SCO Customer,

UnixWare 7.1.4 Maintenance Pack 3 is a required update for your UnixWare 7.1.4 system and should be applied at your next maintenance period. This Maintenance Pack contains all the features and fixes delivered in previous UnixWare 7.1.4 Maintenance Packs, as described in this document.

Contents

I. Before Installing the Maintenance Pack

Please read the following notes and recommendations before you begin installing the Maintenance Pack.

1. The UnixWare 7.1.4 Maintenance Pack 3 should only be installed on:

   UnixWare 7.1.4

2. If you are performing an in place upgrade to UnixWare 7.1.4 from UnixWare 7.1.1, UnixWare 7.1.2 (Open UNIX 8.0.0), or UnixWare 7.1.3, you must be sure to reboot the system after upgrading to Release 7.1.4 and before installing this maintenance pack.

3. The maintenance pack consists of the **Maintenance Pack Set**, plus a number of updated packages that are separate from the Maintenance Pack Set, as shown in the following table. A green version number in the table indicates when a new version of a package was introduced.

uw714mp3 - UnixWare 7.1.4 Maintenance Pack 3 Set
The **uw714mp3** set installs these 4 packages:

Package Name and Description			**UW714**	**MP1**	**MP2**	**MP3**
1	uw714m3	UnixWare 7.1.4 Maintenance Pack 3 package				8.0.2
2	libc	Runtime C Library	8.0.2	8.0.2a	8.0.2b	8.0.2c
3	libthread	Runtime Thread Library	8.0.2	8.0.2a	8.0.2a	8.0.2a
4	pam	Pluggable Authentication Modules	New in MP1	0.77	0.77	0.77a

UnixWare Packages
These packages and the Open Source packages that follow can be installed after you install **uw714mp3**:

Package Name and Description			**UW714**	**MP1**	**MP2**	**MP3**
1	nics	Network Infrastructure and Configuration Subsystem	8.0.2	8.0.2a	8.0.2b	8.0.2c
2	nd	Network Drivers	8.0.2		8.0.2b	8.0.2c
3	ldap	Lightweight Directory Access Protocol services	8.0.1		8.0.1a	8.0.1a
4	libosr	Runtime OpenServer Libraries	8.0.2		8.0.2a	8.0.2a
5	uccs	OUDK Optimizing C Compilation System	8.0.2	8.0.2a	8.0.2b	8.0.2c
6	uw7mpdoc	Updated Guides and Manual Pages	New in MP1	7.1.4a	7.1.4a	7.1.4a
7	basex	X11R6 Base X Runtime System	8.0.2		8.0.2a	8.0.2b
8	xserver	X11R6 X Server	8.0.2	8.0.2a	8.0.2b	8.0.2c
9	xclients	X11R6 X Clients	8.0.2		8.0.2a	8.0.2.a
10	xcontrib	X11R6 Contributed X Clients	8.0.2	8.0.2a	8.0.2b	8.0.2c
11	xdrivers	X11R6 Graphics Drivers	8.0.2		8.0.2a	8.0.2b

Open Source Packages

Package Name and Description			**UW714**	**MP1**	**MP2**	**MP3**
1	zlib	General Purpose Data Compression Library	1.2.1		1.2.1-01	1.2.3
2	openssl	OpenSSL	0.9.7c	0.9.7d	0.9.7d	0.9.7i
3	openssld	OpenSSL Documentation	0.9.7c	0.9.7d	0.9.7d	0.9.7i
4	db	Berkeley DB Library	4.1			4.1.25
5	libpng	PNG (Portable Network Graphics) Library	1.2.5		1.2.7	1.2.7
6	tiff	TIFF Library and Utilities	3.5.7			3.7.3
7	gs	ESP Ghostscript	7.05.6			7.07.1
8	cups	Common Unix Printing System	1.1.19-01	1.1.19-02	1.1.19-03	1.1.19-03
9	foomatic	Foomatic Filters and PPDs	3.0.0-01	3.0.0-02	3.0.2	3.0.2
10	hpijs	HP Inkjet Printer Driver	1.5	1.5-01	1.5-02	1.5-02
11	gzip	GNU file compression utilities	1.2.4			1.3.5

15	samba	Samba	3.0.0	3.0.4	3.0.10	3.0.10
16	squid	Squid Caching Proxy Server	2.4.STABLE7		2.5.STABLE7	2.5.STABLE12
17	modjk1	mod_jk2 for Apache 1	New in MP1	2.0.4	2.0.4	2.0.4
18	mysql	MySQL multithreaded SQL database server	3.23.49			4.1.11
19	mozilla	Mozilla 1.7.12	1.2.1b			1.7.12
20	ipf	IP Filter	New in MP2		4.1.3	4.1.3a

4. In addition to the packages in this Maintenance Pack, additional new and updated packages (such as device drivers and Java) are available separately from the UnixWare 7.1.4 Support Download Site at: http://www.sco.com/support/update/download/product.php?pfid=1&prid=6.

5. An **install.sh** script is provided to simplify installation, as described in the Installing the Maintenance Pack section below. Use of this script is highly recommended.

   The **install.sh** script installs the following:

   - The **uw714mp3** set.

     Installing **uw714mp3** will update the **libc** and **libthread** runtime libraries as well as installing the **uw714m3** and **pam** packages. The runtime libraries, once installed, are not removable.

   - The **uw7mpdoc** package.

   - Newer versions of the updated packages listed above, provided earlier versions of these packages are already installed on your system.

   Alternatively, with care you can install the packages individually. However, you should note the following:

   - The **uw714mp3** set is required for all systems.

   - The following packages are required to be updated, that is you must install them if you have an earlier version installed on your system to maintain system integrity:

     cups
     openssh
     samba
     xcontrib

   - The following packages are strongly recommended:

     basex
     cdrtools
     foomatic
     gzip
     libpng
     MySQL
     mozilla
     nd
     nics
     openssl
     squid
     tiff
     uccs
     xclients
     zlib

xserver
xdrivers

- All other packages are optional.

If you did not install some of the above packages when initially installing UnixWare 7.1.4, you can do so using the **install.sh** script. You do not need to first install the original UnixWare 7.1.4 versions. Please refer to the Installing the Maintenance Pack section below.

6. A **mkiso.sh** script is provided with this maintenance pack to create custom maintenance pack ISO image files and/or CDs from the original maintenance pack ISO image file or CD, as described in the Custom CD Creation Instructions section below.

   Notes:
   - To use this feature, you need the **cdrtools** package installed.
   - To burn the custom ISO image file, you need a writable CD drive and CD Media.

7. This maintenance pack supercedes and obsoletes:

uw714mp1	UnixWare 7.1.4 Maintenance Pack 1 Set
uw714mp2	UnixWare 7.1.4 Maintenance Pack 2 Set
ptf9050	UnixWare 7.1.4 Licensing Supplement
ptf9051	UnixWare 7.1.4 Maintenance Pack 2 Supplement

   These packages and sets do not need to be removed prior to installing **uw714mp3**, and the installation of **uw714mp3** will lock down these packages so that they will no longer be removable.

8. If your system was originally installed with a release prior to UnixWare 7.1.3 and has the obsolete **scohelp** package installed, we recommend removing **scohelp** before you add the MP. This will ensure the full benefit of the security enhancements in the MP (changes to numerous file and directory permissions). To see if **scohelp** is installed, enter the following shell command:

```
# pkginfo scohelp
```

   To remove the package, enter the following two commands as *root*:

```
# /etc/scohelphttp stop
# pkgrm scohelp
```

9. If you install a package (e.g., **acp**) from the UnixWare media kit that has been updated by the maintenance pack on a system with the maintenance pack installed, you will see the following warning message:

```
The <acp> package was installed after installing the <uw714m3> package.

WARNING:
The <uw714m3> package contains updates to the above package(s).

Please reinstall the <uw714m3> package.  Failure to do so may leave
your system in an inconsistent state.
```

   This warning message will be displayed after every **pkgadd** until you reinstall the **uw714m3** package. To do this, mount the maintenance pack CD and type the following two commands as *root*:

```
# pkgadd -d /mount_point/images/uw714mp3.image uw714m3
# shutdown -i6 -g0 -y
```

10. For a list of the major features and improvements delivered with this maintenance pack, please see the Highlights of this Maintenance Pack section below.

11. For a list of issues that this maintenance pack addresses, please see the Problems Fixed in this Maintenance Pack section below.
12. For a list of known issues with this maintenance pack, please see the Maintenance Pack Notes and Limitations section below.
13. If you have questions regarding this supplement, or the product on which it is installed, please contact your software supplier or support representative.

II. Installing the Maintenance Pack

1. Log in as *root*.
2. Do one of the following:
   - **If you are installing the maintenance pack from CD**, insert the maintenance pack CD into the primary CD drive and enter:

     ```
     # mount /dev/cdrom/cdrom1 /install
     ```

   - **If you are installing this maintenance pack from the web**, download the *uw714mp3.iso* file to your server from:

     http://www.sco.com/support/update/download/release.php?rid=126

     In the directory where you downloaded the uw714mp3.iso file, enter:

     ```
     # mount `marry -a uw714mp3.iso` /install
     ```

3. Change directory to */install*:

   ```
   # cd /install
   ```

4. Do one of the following:

   A. **To install the required uw714mp3 set and the updated packages on your system, enter**:

   ```
   # ./install.sh [-nv]
   ```

   This will show you a menu screen listing the names of the packages that are part of this maintenance pack. By default:

   - The following are selected for installation: **uw714mp3**, **uw7mpdoc**, and any packages whose earlier versions are already installed.
   - If an earlier version of a package in the MP is *not* already installed on your system, then that package is *not* selected for installation.
   - If a later version of a package in the MP is already installed on your system, then that package is not listed in the menu.

   The menu screen displays ten packages at a time:

   1. Examine the selected packages on the first screen and make any changes desired.
   2. Select "Apply" to display the next screen of packages.
   3. Continue making any changes needed on each screen and select "Apply" to display the next screen.
   4. Select "Apply" on the final screen to install the selected packages.

   The optional **-n** (non-interactive) flag skips the menu screen and proceeds to install the default selection of packages. The optional **-v** (verbose) flag provides more status information during the installation.

B. **To individually install packages and sets, enter**:

```
# ./install.sh [packages]
```

where *packages* can be any of the packages listed in Section I.

5. After all desired packages are installed, reboot the system by typing:

```
# shutdown -i6 -g0 -y
```

III. Removing the Maintenance Pack

1. Log in as *root*
2. To remove the maintenance pack set (except for its library packages, which are not removable), type:

```
# pkgrm uw714mp3
```

Notes:
- Removal of the **uw714mp3** set is *not* recommended.
- The IP Filter (**ipf**) and Open Secure Shell (**openssh**) packages are functionally dependent on the **uw714m3** package. These packages will not work if **uw714m3** is removed.

3. To fully restore your system to its prior state, reinstall the UnixWare 7.1.4 media kit versions of all packages updated by the Maintenance Pack.

Note: Removal of the updated packages is not recommended.

4. After all the packages are removed, reboot the system by typing:

```
# shutdown -i6 -g0 -y
```

IV. Custom CD Creation Instructions

1. Follow steps 1 to 3 of section II.
2. Enter:

```
# ./mkiso.sh
```

This will ask you the name of the ISO image file. The default is */uw714mp3.iso*.

After entering the ISO path name, a menu screen listing the names of the packages that are part of this maintenance pack is displayed.

By default all packages are selected.

Deselect the packages that you want to exclude from your custom CD. and press "Apply" to continue. Since the menu screen can only display ten packages at a time, pressing "Apply" will show the next list of packages. Pressing "Apply" on the final screen will create the CD ISO image file.

Note: The **uw714mp3** package cannot be deselected.

3. To burn the ISO image file, insert the CD media in your writeable CD drive and enter:

```
# cdrecord -v -dao -speed=16 -fs=10m -dev=device -driveropts=burnfree filename
```

where *device* is the SCSI target for the CD drive. and *filename* is the name of your custom ISO image file.

Use **cdrecord -scanbus** to get device information. Please refer to the **cdrecord**(1) manual page for details.

V. Highlights of this Maintenance Pack

The following summarizes the major features and improvements in this Maintenance Pack. They are listed in the order in which the features were introduced in this and previous UnixWare 7.1.4 Maintenance Packs.

Also see the Problems Fixed in this Maintenance Pack for the complete list of changes made in this Maintenance Pack.

A. Maintenance Pack 1 Highlights
B. Maintenance Pack 2 Highlights
C. Maintenance Pack 3 Highlights

Maintenance Pack 1 Highlights

Encrypting Filesystems

A new encryption feature has been added to the **marry**(7) driver. Using the **marry**(1M) command, an empty regular file is associated with a block special device name, and encryption is enabled on the file. A file system is created on the block special device using the **mkfs**(1M) command, and the block special device is mounted using the **mount**(1M) command. Once mounted, all data written to the file is encrypted using the 128 bit Advanced Encryption Standard (also known as 128bit AES and the Rijndael block cipher); all data read from the file is decrypted. A simple example follows:

1. In the commands below in this procedure, *regfile* is the full pathname to the regular file that will contain the encypted file system. Make sure that *regfile* does not exist; if it does, rename or delete it before continuing. Create *regfile* and assign appropriate permissions and ownership, as in this example:

```
# touch regfile
# chmod 660 regfile
# chown root regfile
# chgrp appgrp regfile
```

2. In the commands below in this procedure, *mountpoint* is the full pathname of the directory to be used to mount the file system. Make sure that *mountpoint* is an empty directory; move or delete any data residing there before continuing. If *mountpoint* does not exist, create it and assign appropriate permissions and ownership, as in this example:

```
# mkdir mountpoint
# chown root mountpoint
# chgrp appgrp mountpoint
# chmod 750 mountpoint
```

3. Marry a block special device to *regfile* and enable encryption on the device:

```
# cryptfs=`marry -a -b blksz -c "passphrase" regfile`
```

   In the example above, the output of the **marry** command (which can be quite long depending on the path used

for *regfile*) is assigned to the **$cryptfs** environment variable; this is done only to simplify typing the commands in the next step.

The *blksz* is the maximum size of the married device, in 512-byte blocks, *plus 5 blocks for encryption information*. So, if you want a file system with a maximum size of 10000 512-byte blocks, use 10005 for *blksz*. The *passphrase* (similar to a password, but longer) is used to generate the keys that encrypt and decrypt the contents of *regfile*. See the **marry**(1M) manual page for a full explanation of *passphrase*.

4. Make and mount the file system:

```
# mkfs -F vxfs $cryptfs blksz-5
# mount $cryptfs mountpoint
```

Note that **$cryptfs** is the output of the **marry** command from the previous step. Also note that the block size used in the **mkfs** command must be 5 blocks less than the *blksz* used in the previous **marry** command.

Please note that an encrypted file system requires more system overhead than a regular file system; this can have a significant effect on performance, depending on the intended use of the encrypted file system. See the **marry**(1M) and **marry**(7) manual pages for more information, including the limitations of this interface.

Perl Module mod_jk1 for Apache and Tomcat

The Perl module **mod_jk1** is used to connect an Apache Web Server to a Tomcat Java Application Server, to provide Web access to Java Applications. Apache and Tomcat are part of the SCOx Web Enabling and Web Services Substrate software, distributed as part of Release 7.1.4. Information on configuring **mod_jk1** can be found on the Apache Jakarta Project server at: http://jakarta.apache.org/tomcat/connectors-doc/jk2/jk/quickhowto.html. Tomcat documentation can be found on the Tomcat website at http://jakarta.apache.org/tomcat, and Apache documentation is available from the default Apache server running on UnixWare on port 80 (**http://localhost:80**).

Pluggable Authentication Modules (PAM)

The Pluggable Authentication Modules (PAM) feature allows an administrator to manage the authentication policy used by all applications that support PAM without making any changes to those applications. PAM is implemented through:

- changes to the kernel to support PAM modules
- standard PAM modules in the PAM libraries, for use in authentication-related code in applications
- changes to critical system utilities, such as **login**, to support PAM
- changes to applications, such as Samba, to support PAM

Please see the PAM documentation for more information.

Samba 3.0 - Multibyte and PAM-enabled

The **samba** package provides an update to the Samba 3.0 distributed with Release 7.1.4. This version is enabled for the Pluggable Authentication Modules (PAM) feature, the Name Service Switch (NSS) feature, and also supports the use of multibyte characters for Asian locales. If you install *and enable* PAM, you must also install the PAM-enabled Samba 3.0 package, since the version of Samba distributed with Release 7.1.4 (and other previous versions) will no longer work once PAM is enabled.

Maintenance Pack 2 Highlights

ATI Radeon ES1000/RN50 Graphics Card Support
Updated Drivers
New Open Source Packages

IP Filtering

IP Filter 4.1.3 is an advanced open source filtering package which provides both firewall and network address translation (NAT) services. It is the most common filtering package supported across different implementations of the UNIX System. Documentation for IP Filtering is provided on the UnixWare 7.1.4 Documentation Web Site at http://uw714doc.sco.com/en/NET_tcp/ipfintro.html.

New lsof Command

The **lsof** command version 4.73 lists information about currently open files. Executing **lsof** as *root* with no options displays a line describing each file that has been opened by every currently running process; this list can be large. **lsof** supports the following options:

```
lsof [-?abChlnNoOPRstUvV] [+|-c c] [+|-d s] [+|-D D] [+|-f[cfgGn]]
 [-F [f]] [-g [s]] [-i [i]] [-k k] [+|-L [l]] [-m m] [+|-M] [-o [o]]
 [-p s] [+|-r [t]] [-S [t]] [-T [t]] [-u s] [+|-w] [-x [fl]] [--] [names]

Defaults in parentheses; comma-separate set (s) items; dash-separate ranges.
  -?|-h list help
  -a AND selections (OR)
  -b avoid kernel blocks
  -c c  cmd c, /c/[bix]
  +c w  COMMAND width (9)
  -C no kernel name cache
  +d s  dir s files
  -d s  select by FD set
  +D D  dir D tree *SLOW?*
  -D D  ?|i|b|r|u[path]
  -i select IPv[46] files
  -l list UID numbers
  -n no host names
  -N select NFS files
  -o list file offset
  -O avoid overhead *RISK
  -P no port names
  -R list paRent PID
  -s list file size
  -t terse listing
  -T disable TCP/TPI info
  -U select Unix socket
  -v list version info
  -V verbose search
  +|-w  Warnings (+)
  -- end option scan
  +f|-f  +filesystem or -file names
  +|-f[cfgGn] Ct,Fstr,flaGs,Node
  -F [f] select fields; -F? for help
  -k k   kernel symbols (/stand/unix)
  +|-L [l] list (+) suppress (-) link counts < l (0 = all; default = 0)
  -m m   kernel memory (/dev/kmem)
  +|-M   portMap registration (-)
  -o o   o 0t offset digits (8)
  -p s   select by PID set
  -S [t] t second stat timeout (15)
  -T fqs TCP/TPI Fl,Q,St (s) info
  -g [s] select by process group ID set and print process group IDs
  -i i   select by IPv[46] address: [46][proto][@host|addr][:svc_list|port_list]
  +|-r [t] repeat every t seconds (15); + until no files, - forever
  -u s   exclude(^)|select login|UID set s
  -x [fl] cross over +d|+D File systems or symbolic Links
  names  select named files or files on named file systems
```

For the current **lsof** manual page, please see: ftp://lsof.itap.purdue.edu/pub/tools/unix/lsof/lsof_man. A FAQ is available at: ftp://lsof.itap.purdue.edu/pub/tools/unix/lsof/FAQ.

PC Card Wireless Support

Laptop PC Card support has been updated to include CardBus Card support. The following NIC drivers have been updated to include PC Card support: **d21x**, **e3E** and **nat**.

The following new adapters are now supported, including CardBus NICs and selected PRISM II Wireless PC Card NICs:

```
3Com EtherLink III 3C589C 0101058906
3Com EtherLink III 3C589D 0101058906
3Com 10Mbps LAN PC Card 3CCE589EC
3Com 10Mbps LAN PC Card 3CXE589DT
3Com 10Mbps LAN PC Card 3CCE589ET
3Com 10/100 LAN PC Card 3C3FE574BT
Intel PRO/100 CardBus II MBLA3300
Intel PRO/100 S Mobile Adapter MBLA3300 C3
Intel PRO/100 CardBus II MBLA3400
Linksys Combo PCMCIA EthernetCard EC2T
Linksys EtherFast 10/100 PC Card PCMPC100
Linksys EtherFast 10/100 CardBus Card PCMPC200
Linksys Wireless-B Notebook Adapter (802.11b)
Netgear 10/100 PCMCIA FA410
Netgear 10/100 PCMCIA Mobile Adapter FA411
Netgear 10/100 CardBus FA510
Netgear 802.11b Wireless PC Card MA401
Socket Communications EA
Socket Communications LP-E
```

Also see Maintenance Pack Notes and Limitations, below, if you are installing the Maintenance Pack on a laptop that already has a PC Card or CardBus NIC installed.

ATI Radeon ES1000/RN50 Graphics Card Support

Support for the ATI Radeon ES1000/RN50 video card has been added to the xdrivers-8.0.2b package.

Updated Drivers

Please see the description of the updated printer drivers, updated network drivers, and the updated X Drivers provided with Maintenance Pack 2, in Section VI.B, below.

New Open Source Packages

Please see the package table in Section I for a list of the updated and new open source packages provide in MP2.

Maintenance Pack 3 Highlights

Dual Core Support -- Intel and AMD

Multiple core processors have two or more processor cores in each physical package, continuing the trend started with hyperthreading, but offering enhanced parallelism and improved performance due to additional processor cores.

Multiple processor cores are automatically detected and utilized if they are available. However, hyperthreaded

processors are not utilized unless the administrator specifically requests their use. No additional CPU licenses are required to use either multiple processor cores or hyperthreaded processors.

The use of multiple processor cores can be disabled with the boot parameter "MULTICORE=N" entered at the boot prompt or added to the "/stand/boot" file. Having multiple core support enabled has no effect on systems that do not have multiple core processors. If the use of multiple processor cores is explicitly disabled with the "MULTICORE=N" boot parameter, then the use of hyperthreaded processors is also disabled.

Hyperthreaded processor support is still disabled by default. Support for hyperthreaded processors can be enabled with any of the following boot parameters:

```
ENABLE_HT=Y
HYPERTHREAD=Y
ENABLE_JT=Y
```

Enhanced Wireless Support

The **Intel Centrino Wireless driver** (**ipw**) has been added, and supports the Intel PRO/Wireless 2200BG built-in laptop network card.

PAM Updated for LDAP

A new PAM module (**pam_ldap**) has been added that allows authentication via PAM against an LDAP Server. OpenLDAP includes two new files: */usr/lib/security/pam_ldap.so* and */usr/lib/nss/ldap.so*. These two files together can be used to provide authentication against an OpenLDAP server. For an explanation of using LDAP and PAM, please see http://www.tldp.org/HOWTO/LDAP-Implementation-HOWTO/pamnss.html.

Updated Drivers

Please see the Drivers section for Maintenance Pack 3 in Section VI.C, below.

New Open Source Packages

Please see the package table in Section I for a list of the updated and new open source packages provide in MP3.

Single Certification with OpenServer 6

Changes have been made to the kernel and libraries that support running binaries that were created using the SCO OpenServer 6 Development System in "-K udk" mode.

VI. Problems Fixed in this Maintenance Pack

A. Problems Fixed in Maintenance Pack 1:

```
The UnixWare 7.1.4 Maintenance Pack 1 set (uw714mp1) contains the
following fixes. These fixes are also included in UnixWare 7.1.4
Maintenance Pack 3 set (uw714mp3).

o uw714m1 package fixes:
```

Feature and usability enhancements:

1. The following UnixWare 7.1.4 functionality is now provided:

   o Pluggable authentication modules (PAM) support
   o Encrypted file system support

   These features are described in the online documentation that is provided with the uw7mpdoc package that accompanies this maintenance pack. See the "New Features and Notes" section of the online documentation.
   fz528611 fz529097

2. Intel microcode updates.
   erg712621/ptf9050/fz529619

3. kcrash macros updates.
   fz529663

4. Additional source files for DBA usage with MySQL provided with the SCOx enablement package. Modified Makefile, eelsdba_mysql.c, initdb.mysql and README are provided for use with latest MySQL package.
   fz529851

5. Enabled large file support in compress.
   fz529876

Security improvements:

6. SECURITY: Some files and directories were created incorrectly allowing write permission to arbitrary users. Some system daemons were running with a file creation mask (umask) set to 0.
   fz528862

7. SECURITY: Security vulnerability issues in TCP are fixed according to this IETF draft:
   http://www.ietf.org/internet-drafts/draft-ietf-tcpm-tcpsecure-00.txt
   erg712598/fz529384

8. SECURITY: Two new inconfig tunables have been introduced to address the TCP Rose Attack:

   o ip_maxfragpackets:
     This is the maximum number of fragmented packets that IP will accept. The default is 800.

   o ip_maxfragsperpacket:
     This is the maximum number of fragments per packet that IP will accept. The default is 16.

   erg712605/fz529414 SCOSA-2005.14

Reliability improvements:

9. Fixed kernel panic on errant umem_free() in [g|s]etgroups_sco.
   fz528775

10. Fixed a memory corruption bug caused by not stopping netbios when the system was brought to init state 1.
    ptf9050b/fz529565

11. Fixed process hangs due to race between exiting children and SIGCLD processing in the parent.
    erg712596/fz529361

Networking improvements:

12. Changed use of types u_[short,int,long] to u[short,int,long]_t in <netinet/tcp.h> since the former are not always defined.
    fz529581

13. The SHUT_RD, SHUT_WR, and SHUT_RDRW macros in <sys/socket.h> are defined only when at least one XOPEN-ish feature test macro is defined. This is counter to our "everything visible by default" model for headers.

The TOG SUS says that SHUT_* macros can be defined in general, so there's no reason not to define these with no conditional inclusion coverage.
fz529698

14. Under some circumstances, ppp could go into an infinite loop of read calls in the libnsl ics_read_data() routine.
erg712620/fz529611

Installation tools improvements:

15. By the time pkgadd executes the preinstall script of a package, it has already updated the contents file with the information from the package's pkgmap file. Hence if the preinstall script is terminated for some reason, the contents file is left in a bad state - the files are not installed on the system but they are present in the contents file. This has been fixed so that the contents file is not updated until the files are installed.
fz519105

16. Fixed a problem where pkginstall, pkgremove and installf can destroy the software contents file if it is already locked by another process.
fz198541

Licensing improvements:

17. The license policy daemon ignores custom licenses from earlier releases. For example, if your system license had previously included extra users, not separately licensed but included in your original, those users would be ignored. This has been fixed.
ptf9050a/fz529560

o Runtime C Library (libc) version 8.0.2a fixes:

18. Bad parsing of some special strings in string-to-floating code.
fz529765

o Runtime Thread Library (libthread) version 8.0.2a fixes:

19. Oracle may hang while starting by going into an infinite loop in libthread's thr_keycreate().
erg712658/fz529884

Additional bug fixes and enhancements were provided with the supplemental packages that were distributed with UnixWare 7.1.4 Maintenance Pack 1. These fixes are also included in the supplemental packages provided with UnixWare 7.1.4 Maintenance Pack 3.

o Documentation:

1. The Updated Base System Guides (uw7mpdoc) package, version 7.1.4a, provides documentation for the PAM, encrypted file system, modjk1, and Samba features delivered with uw714mp1 and its supplemental packages.

o PAM:

2. The following supplemental packages have been updated to enable support for PAM. They can only be installed if the pam package (contained in uw714mp3 set) is installed:

```
cups     - Common Unix Printing System, version 1.1.19-02
openssh  - Open Secure Shell, version 3.8.1p1
samba    - SMB based file/printer sharing, version 3.0.4
xcontrib - X11R6 Contributed X Clients, version 8.0.2a
```

o The Foomatic Filters and PPDs (foomatic) package, version 3.0.0-02, and the HP Inkjet Printer Driver (hpijs) package, version 1.5-01, contain this fix:

3. Fixed obscure corruption of a few data files.
fz529615

o The Netdriver Infrastructure and Configuration Subsystem (nics) package, version 8.0.2a, contains this fix:

4. A time delay of 1 sec in dlpiclose() was causing some applications, e.g. getmany (accessing mib-2 table) to consume large amounts of CPU time. This time delay ensured that all in-transit packets were processed before closing the SAP.

   This delay is removed and the code reworked to use message based synchronization during closedown.

   dlpiclose() now constructs a M_CTL packet containing a message of type dl_ctlmsg_t. This message contains DLPI primitive set as DL_CLOSESAP and a pointer to the SAP structure.

   This message is queued at the DLPI lower read queue so that dlpilrsrv will handle it. It then goes to sleep. When dlpilrsrv receives this message, it is assured that all messages before it have been sent upstream, i.e., there are no in-transit packets. dlpilrsrv signals dlpiclose to close the SAP.

   erg712282/fz526486

o The Open Secure Shell (openssh) package, version 3.8.1p1, contains these fixes:

5. OpenSSH has been updated from version 3.7.1p2 to 3.8.1p1 and support for PAM has been enabled.

   Please see the openssh website for the list of changes.
   http://www.openssh.com/

   fz528611

6. SECURITY: OpenSSH only gives significance to the first 8 characters of a password.
   erg712648/fz529827 SCOSA-2005.19

o The OpenSSL - Secure Sockets Layer / TLS Cryptography Toolkit (openssl) package, version 0.9.7d, contains this fix:

7. SECURITY: OpenSSL has been updated from version 0.9.7c to 0.9.7d to fix several security issues with the earlier version.

   Please see the openssl website for the list of changes.
   http://www.openssl.org/

   erg712602/fz529411 SCOS-2005.7

o The OpenSSL Documentation (openssld) package, version 0.9.7d, provides the updated documentation for the openssl package version 0.9.7d.

o The SMB based file/printer sharing (samba) package, version 3.0.4, contains these fixes:

8. Samba has been updated from version 3.0.0 to 3.0.4 to enable PAM and to provide multibyte support.

   Please see the samba website for the list of changes.
   http://www.samba.org/samba/

   fz529665

9. Swat server status page shows smbd "not running" even when it is.
   fz528969

o The OUDK Optimizing C Compilation System (uccs) package, version 8.0.2a, contains these fixes:

10. With the introduction of NSS, SCO has changed some existing APIs and added some new APIs to support NSS. Customers building binaries that use these APIs will find that their compile will fail with undefined symbol references similar to the following:

Undefined symbol	first referenced in file
getspnam_r	libperl.so
getpwent_r	libperl.so
getgrent_r	libperl.so

Note:
This problem is only seen in systems upgraded from earlier UnixWare releases to UnixWare 7.1.4.

11. C compiler bug fixed. In -Xt mode, the compiler may incorrectly attempt to combine two typedef's that are not numeric types.
erg712635/fz529721

12. Make command bug fixed. $(XD:str=rep) broken, where X is any of the @*<%? special characters.
erg712665/fz529930

o The X11R6 X Server (xserver) package, version 8.0.2a, contains this fix:

13. SECURITY: Some files and directories were created incorrectly allowing write permission to arbitrary users. Some system daemons were running with a file creation mask (umask) set to 0.
fz528862

o The Additional Modules for Perl (modjk1) package, version 2.0.4, contains this fix:

14. Provides the modjk connector for Apache 1 and Tomcat. Apache 2 users do not need this package.

Notes:
o This package is not installed by default.
o This package will not conflict with modjk for Apache 2 & Tomcat as the library is installed in a different location.

fz529629

B. Problems Fixed in Maintenance Pack 2:

The UnixWare 7.1.4 Maintenance Pack 2 set (uw714mp2) contains the following fixes. These fixes are also included in UnixWare 7.1.4 Maintenance Pack 3 set (uw714mp3).

o uw714m2 package fixes:

Feature and usability enhancements:

1. Updated Laptop PC Card support to include CardBus support.
fz529602

2. Updated /sbin/p6update to support new Intel Prescott and Nacona processors. Includes additional microcode updpates.
fz530177

3. Enhanced /etc/hw command to decode Pentium 4 cache size information and system memory sizes in excess of 4Gb.
fz525623
fz528909

4. Added lsof command version 4.73.

Lsof is a UNIX-specific tool. Its name stands for LiSt Open Files, and it does just that. It lists information about files that are open by the processes running on a UNIX system.

The lsof provided is compiled with the following flags:
-DINKERNEL -Kthread -Kalloca -O2

See the complete copyright notice at the end of this file.
fz530110

5. Increased the number of users from 1 to 2 for the default Business Edition license.
fz530379

6. Added the Japanese Gaigi character definitions to Japanese locales.
   erg712726/fz530392

7. For X11R6 applications, allow the NumLock key to be used with Motif
   accelerator and mnemonic keys for pulldown menus. To enable this
   feature, set the environment variable "XMNUMLOCK=ALL" for the
   process.
   erg712703/fz530229

Security improvements:

8. SECURITY: A new file system tunable, CHROOT_SECURITY is provided
   to protect against a known exploit for escaping from a chroot
   prison. The new tunable is described in /etc/conf/dtune.d/fs and
   defined in /etc/conf/mtune.d/fs. Protection is provided by the
   default value of 1 but traditional behavior may be obtained by
   setting CHROOT_SECURITY to 0, and rebooting the system.
   erg712509/fz528555 SCOSA-2005.2

9. SECURITY: ICMP error messages are discarded for TCP connections if
   TCP sequence number in ICMP payroll is not in the range of the
   data already send but not yet acknowledged.
   erg712758/fz530661

10. SECURITY: Fixed the Common Desktop Environment dtlogin XDMCP Parser
    Remote Double Free vulnerability.
    erg712592/fz529303 SCOSA-2005.18

11. SECURITY: Fixed the following Denial of Service vulnerability.
    When the NFS mountd service is run by inetd and an NFS mount related
    request is received from a remote (or local) host, inetd will
    repeatedly create the mountd process and as a result increasingly
    consume memory. This problem also exists for the following inetd
    services: ypupdated, rusersd, sprayd, and walld.

    To fix this, the mountd service is updated from a "dgram" service to
    a "tli" service. The socket_type (in /etc/inet.d/inetd.conf) is
    also changed from "dgram" to "tli" for the following inetd
    services: mountd, ypupdated, rusersd, sprayd, and walld.
    erg712731/fz530479 SCOSA-2005.1

12. SECURITY: An upgrade to the KAME implementation of internet key
    exchange (IKE) daemon implementation which includes several
    security fixes.
    erg712650/fz529836 SCOSA-2005.10

Reliability improvements:

13. Fixed kernel panic caused by Merge trying to save FPU state when
    FPU hasn't been used.
    fz529860

14. Fixed various bugs in fork that in turn could lead to kernel panics in
    priocntl. The fixes had to do with ensuring that per-lwp properties
    were inherited consistently across a fork.
    fz529463

15. Fixed kernel panic that can sometimes occur due to race condition
    between fdetach of a named pipe and the last close on the pipe's
    file descriptors.
    erg711929/fz519727

16. Fixed kernel panic and kernel memory corruptions caused by an
    erroneous pointer left in a STREAMS lower multiplexor queue
    structure during execution of an I_LINK or I_PLINK ioctl.
    erg712470/fz528449

17. Fixed deadlock that can occur if an NMI occurs on one CPU at the
    same time that another CPU takes a clock interrupt and attempts to
    recalibrate the clock.
    erg712722/fz530382

Networking improvements:

18. Fixed bugs in the scoadmin dhcp and address allocation managers
    that cause tcl failures and hangs.

fz526860
fz528398
fz528404
fz528650
fz529146
fz529522

19. For /dev/tcp, /dev/udp and other related device nodes, permission is given to root to change access and modification times, and to change mode, uid and gid if they are different from the current ones.
erg712672/fz528399

20. Fixed IP packet filtering.
erg712619/fz529605

21. Fixed race between tcp input processing and tcp close processing.
erg712585/fz529161

22. The netstat -I <interface> <interval> command displays output incorrectly, if the machine gets a lot of packets in a particular interval.
erg712663/fz529916

23. System gets many "Out of stream" messages in osmlog and kernel panics afterwards.
erg712707/fz530251

24. SNMP time ticks are being interpreted as signed 32-bit integers instead of unsigned 32-bit integers
erg712732/fz530366

25. An errant assumption about the maximum size of tcp/ip header including the MAC header and the STREAM headers would not exceed 256 bytes caused the system to write past the allocated space. The allocation optimization now properly accounts for the MAC header if it does not exceed the 256 byte KMA pool size.
fz530654

26. There was a namespace conflict within the definition of inet_ntoa. The kernel version is renamed to inet_ntoa_r. This helps to ease porting of open source applications to UnixWare.
fz529706

27. Changes to ip_var.h to allow porting of open source applications without requiring the inclusion of some UnixWare-specific headers.
fz529708

28. Moved _tcpconn and tcp_dbg_hdr data structures and associated defines from tcp.h to tcp_var.h to allow porting of open source applications without requiring the inclusion of some UnixWare-specific headers.
fz530909

USB improvements:

29. Certain USB keyboards exhibit a jitter that is usually seen as the repetition of a previous character.
erg712294/fz527741

30. Fixed a potential problem with newer EHCI USB controllers that are controlled by the system BIOS. The visible symptom is that devices attached to the EHCI ports of certain systems won't work.
fz530306

31. Low and full speed USB devices attached directly (i.e. not via a USB 2.0 hub) to an EHCI controller will get a message logged to the console 'Device reset timeout during enumeration!' when they are discovered. The message is benign; the devices work as expected. This fix eliminates the cause of the distracting message.
fz530377

32. Fixed bug in UDI bridge mapper that caused shared PCI interrupts to remain un-acknowledged during USB host controller initialization leading to system hangs.
erg712677/fz530090
erg712699/fz530174

33. Attempting to autoconfigure a USB mouse via the mouseadmin command did not work properly, and the mouse test would always fail. This problem would only be encountered by those adding or switching to a USB mouse, post ISL, and attempting to autoconfigure it through mouseadmin.
    fz530587

Motif library and X improvements::

34. Fixed a bug where the change of background of the Motif Scale widget with XtSetValues has no effect if the widget was not realized yet.
    erg712682/fz530146

35. Fixed the XmATTACH_OPPOSITE_FORM attachment in the children of a Form widget using the incorrect sign of the value, which causes the form to resize itself to become smaller and smaller.
    erg712697/fz530166

36. Fixed the display of the Japanese messages in programs based on the Athena widgets.

    Note:
    Portions of this fix are contained in the xserver, xclients, and xcontrib packages. These packages must be installed or the commands will stop working in Japanese!

    erg712661/fz529890

Misc improvements:

37. Changes to acpi and mps drivers to recognize pci devices that were previously not found. Includes an upgrade to the latest version of the acpi driver.
    fz530205
    erg712706/fz530250

38. Online and offline of processors may work incorrectly on systems where the processors report more than one logical processor per physical package when hyperthreading is disabled in the system BIOS.
    fz530165

39. Fixed problems caused by the Intel ICH3-S chipset occasionally returning bad real-time clock values. Symptom was that some platforms may hang on boot with warning messages from psm_time_spin_adjust.
    erg712593/fz529317

40. Various "off by one" errors fixed in the interval timer code.
    erg712667/fz529962

41. Disksetup's default blocksize does not work with large VxFS file systems.
    erg712615/fz529483

42. Fixed the reserve bitmap buffer setup to wrong channel/snode during VxFS snapshot creation, which caused snapshots to be disabled due to read i/o failures on good drives.
    erg712644/fz529774

43. init failing to change runlevels. There was a race condition in the waitproc function in the init code that has been fixed.
    erg712313/fz527890

44. System hangs on boot - idmknodd last process run. There was a race condition in the waitproc function in the init code that has been fixed.
    erg712607/fz529426

45. Fields incorrectly labeled in rtpm utility in Japanese locale.
    fz530091

46. The auditrpt -f <filename> command is causing segmentation faults on some audit report data files.
    erg712760/fz530410

47. The ap command is causing segmentation fault.

Note: Portion of this fix is in the libc package.

erg712675/fz530046

48. The creatiadb command is not working.
    erg712678/fz530093

49. The ps command will now report NI values as set by nice(2), rather
    than always displaying a 0 in that output column. This is only a
    compatibility measure and does not imply that the value set by
    nice(2) will affect scheduling behavior.
    fz530118

50. Printer manager GUI hangs while adding local printers on a freshly
    installed system.
    fz530092

51. C++ template instantiation fails when object file has non-.o suffix
    To fix this, .ti and .ii suffixes now append to, rather than
    replace, non-.o object suffixes.
    fz530247

52. A function call argument that is an expression with "side effects",
    cannot be used directly more than once when doing function inlining.
    A C++ "? :" expression, in which the third operand (conditionally
    evaluated) created a short-lived temp class object, was incorrectly
    replicated when replacing a multiply-referenced parameter in an
    inlined function.
    fz530178

53. For NIS systems, correct lookup-by-GID failure.

    Note: Portion of this fix is in the libc package.

    fz530952

54. We now have libcrypto.so from openssl package also and it defines
    _des_crypt() which is also defined by libcrypt.so. Updated
    libcrypt.so to use its own definition so that things remain sane.
    fz530438

55. Updated the /usr/lib/apache/conf/httpd.conf file if apache-1.3.29 and
    php-4.3.5 are installed, or the /opt/apache2/conf/conf.d/php4.conf
    file if apache2-2.0.49 and php4-4.3.5 are installed, with:

    AddType application/x-httpd-php .php .php3 .inc .phtml
    AddType application/x-httpd-php-source .phps

    In future, installation of php or php4 should update these files.
    fz529730

56. Fixed Tomcat 4.1.30 start script to implement a nohup.
    In future, this will be fixed in the tomcat package.
    fz530103

57. Fixed the Perl 5.8.3 configuration files to remove build pathnames.
    In future, this will be fixed in the perl package.
    fz530344

58. Fixed a syntax error in Mozilla start script.
    In future, this will be fixed in the mozilla package.
    fz530539

o Runtime C Library (libc) version 8.0.2b fixes:

Note:
All fixes in the libc package are also included in the uccs package.

59. Fixed a memory leak in tzset().
    erg712729/fz530421

60. 61The ap command is causing segmentation fault.
    erg712675/fz530046

61. PAM enabled services do not update syslog correctly.
    fz530185

fz529908

62. For NIS systems, correct lookup-by-GID failure.
fz530952

Additional bug fixes and enhancements are provided with the following packages that are distributed with UnixWare 7.1.4 Maintenance Pack 2. These fixes are also included in the supplemental packages provided with UnixWare 7.1.4 Maintenance Pack 3.

o The Common Unix Printing System (cups) package, version 1.1.19-03:

1. SECURITY: Fixed a Denial of Service vulnerability. It was possible to disable browsing in CUPS by sending an empty UDP datagram to port 631 where cupsd is running.
erg712688/fz530153 SCOSA-2004.15

,

o The Foomatic Filters and PPDs (foomatic) package, version 3.0.2:

2. SECURITY: Foomatic has been updated from version 3.0.0-02 to 3.0.2 to fix a security problem.

Please see the foomatic website for the list of changes.
http://www.linuxprinting.org/foomatic.html

erg712704/fz530505 SCOSA-2005.12

o The HP Inkjet Printer Driver (hpijs) package, version 1.5-02:

3. Updated and new PPD files for non-HP printers from the foomatic-3.0.2 distribution.
erg712704/fz530505

o The Lightweight Directory Access Protocol services (ldap) package, version 8.0.1a:

4. LDAP fails to start with the following error message:
dynamic linker: /usr/lib/ldap/slapd: relocation error symbol not found: ldapdebug_level referenced from /usr/lib/ldap/slapd
erg712679/fz527615

o The Runtime OpenServer library (libosr) package, version 8.0.2a:

5. This version contains an updated libc.so.1 and three new libraries: libm.so.1, libcurses.so.1, and libsocket.so.2.
fz529055

o The PNG (Portable Network Graphics) Library (libpng) package, version 1.2.7:

6. SECURITY: Libpng has been updated from version 1.2.5 to 1.2.7 to fix several security problems.

Please see the libpng website for the list of changes.
http://www.libpng.org/pub/png/libpng.html

erg712684/fz530149 SCOSA-2004.16

o The Network Drivers (nd) package, version 8.0.2b:

7. Updated Intel PRO/100 (eeE8) Network Driver to version 2.9.1.
fz530765

8. Updated Intel PRO/1000 (e1008g) Network Driver to version 7.4.9.
fz530764

9. Updated Broadcom Gigabit (bcme) Network Driver to version 7.5.22.
fz530259

10. The following NIC drivers have been updated to include PC Card support: d21x, e3E and nat.
fz529602

11. The following new adapters are now supported including CardBus NICs and selected PRISM II Wireless PC Card NICs:

3Com EtherLink III 3C589C 0101058906
3Com EtherLink III 3C589D 0101058906
3Com 10Mbps LAN PC Card 3CCE589EC
3Com 10Mbps LAN PC Card 3CXE589DT
3Com 10Mbps LAN PC Card 3CCE589ET
3Com 10/100 LAN PC Card 3C3FE574BT
Intel PRO/100 CardBus II MBLA3300
Intel PRO/100 S Mobile Adapter MBLA3300 C3
Intel PRO/100 CardBus II MBLA3400
Linksys Combo PCMCIA EthernetCard EC2T
Linksys EtherFast 10/100 PC Card PCMPC100
Linksys EtherFast 10/100 CardBus Card PCMPC200
Linksys Wireless-B Notebook Adapter (802.11b)
Netgear 10/100 PCMCIA FA410
Netgear 10/100 PCMCIA Mobile Adapter FA411
Netgear 10/100 CardBus FA510
Netgear 802.11b Wireless PC Card MA401
Socket Communications EA
Socket Communications LP-E

o The Network Infrastructure and Configuration Subsystem (nics) package, version 8.0.2b:

12. System kernel panics under heavy load in dlpi_hwfail_handler. There was race condition in txmon handler.
erg712681/fz530124

o The Open Secure Shell (openssh) package, version 3.9p1-01:

13. OpenSSH has been updated from version 3.8.1p1 to 3.9p1.

Please see the openssh website for the list of changes.
http://www.openssh.com/

14. When sshd is stopped and restarted, it no longer works.
The user trying to get in gets the following message:
Read from socket failed: Resource temporarily unavailable
fz529865

15. Host based authentication does not work with openssh.
fz530102

16. Cannot login to an account with an expired password with openssh.
fz530287

o The Samba (samba) package, version 3.0.10:

17. SECURITY: Samba has been updated from version 3.0.4 to 3.0.10 to fix several security problems.

Please see the samba website for the list of changes.
http://www.samba.org/samba/

erg712735/fz530486 SCOSA-2004.15
erg712754/fz530644

o The Squid Caching Proxy Server (squid) package, version 2.5.STABLE7:

18. SECURITY: Squid has been updated from version 2.4.STABLE7 to 2.5.STABLE7 to fix several security problems.

Please see the squid website for the list of changes.
http://www.squid-cache.org/

erg712610/fz529457 SCOSA-2005.16
erg712740/fz530514

o The OUDK Optimizing C Compilation System (uccs) package, version 8.0.2b:

19. SECURITY: Fixed predictable temporary file creation by the cscope command that can be exploited by any local attacker to remove arbitrary files on the vulnerable file system via the infamous symlink vulnerability.
erg712738/fz530500

20. When doing optimization on functions with exceptionally large code blocks where the total number of arguments passed to calls in

a single block exceeds 8000, the C or C++ compiler may generate incorrect memory addresses for local variables. This problem has only occurred in atypical 4GL generated source code.
erg712757/fz530656

21. Invalid #define of setterm() macro in curses.h.
fz530412

22. When alloca() is used as an argument to another function call, the stack of the current frame may be corrupted such that invalid (saved) register values may be returned to the callee.
fz527215
fz531008

o The General Purpose Data Compression Library (zlib) package, version 1.2.1-01:

23. SECURITY: Fixed a Denial of Service vulnerability. Fixed error handling in the inflate implementation to avoid incorrectly continuing to process in error state.
erg712692/fz530158 SCOSA-2004.17

o The X11R6 Base X Runtime System (basex) package, version 8.0.2a:

24. SECURITY: Fail-soft mechanism is implemented for handling cases where the permissions and/or owner of the /tmp/.X11-unix, /tmp/.ICE-unix, and /tmp/.font-unix directories are not correctly set.

Fail-soft means, if the permission and/or owner is improperly set, the component would try to properly set it. If it is unable to do that, it would generate error/warning message(s), but the component would not fail.

Note: Portions of this fix are contained in the xserver package.

erg712694/fz530161 SCOSA-2005.8

25. Fixed XtAppAddInput() function.
Added missing brackets around XPOLL_READ, XPOLL_WRITE, XPOLL_EXCEPT
erg712671/fz529974

o The X11R6 X Server (xserver) package, version 8.0.2b:

26. Invoking "scoadmin video" on an Intel SE7520JR2 white box server to adjust graphics resolution in either character or graphics mode causes the system console to start blinking, and there is no recovery other than rebooting.
erg712755/fz530648

o The X11R6 Contributed X Clients (xcontrib) package, version 8.0.2a:

27. Fixed warning message from the xtetris command.
fz530182

28. The puzzle command is causing segmentation fault.
erg712700/fz530183

29. The ar command displays incorrect message in Japanese environment.
erg712640/fz529737

o The X11R6 Graphics Drivers (xdrivers) package, version 8.0.2a:

30. Added the Matrox G550 Video Adapter support to the mtx driver.
fz530771

o The IP Filter (ipf) package, version 4.1.3:

31. IP Filter 4.1.3 is an advanced open source filtering package which provides both firewall and network address translation services. It is the most common filtering package supported across different flavors of UNIX. For a complete list of features and services provided, please check the following URLs.

o http://coombs.anu.edu.au/~avalon/
o http://www.obfuscation.org/ipf/ipf-howto.txt

```
fz530132
```

C. Problems Fixed in Maintenance Pack 3:

Feature and usability enhancements

1. **Support for HOPF Serial Device and the following clocks is enabled in NTP demon and utilties.** --

   ```
   o Diem Computime Radio Clock
   o ELV/DCF7000 clock
   o HOPF 6021 clock
   o Meinberg clocks
   o RCC 8000 clock
   o Schmid DCF77 clock
   o WHARTON 400A Series clock
   o VARITEXT clock
   ```

   (ID: 531232:2 ESC: erg712797)

2. **Support for Intel multiple (dual) core processors.**

   Multiple core processors have two or more processor cores in each physical package, continuing the trend started with hyperthreading, but offering enhanced parallelism and improved performance due to additional processor cores.

   Multiple processor cores are automatically detected and utilized if they are available. However, hyperthreaded processors are not utilized unless the administrator specifically requests their use. No additional CPU licenses are required to use either multiple processor cores or hyperthreaded processors.

   The use of multiple processor cores can be disabled with the boot parameter "MULTICORE=N" entered at the boot prompt or added to the "/stand/boot" file. Having multiple core support enabled has no effect on systems that do not have multiple core processors. If the use of multiple processor cores is explicitly disabled with the "MULTICORE=N" boot parameter, then the use of hyperthreaded processors is also disabled.

   Hyperthreaded processor support is still disabled by default. Support for hyperthreaded processors can be enabled with any of the following boot parameters:

   ```
   ENABLE_HT=Y
   HYPERTHREAD=Y
   ENABLE_JT=Y
   ```

   (ID: 532712:3 SLS: ptf9051b)

3. **Support for AMD Dual Core processors.**
   (ID: 532956:2 SLS: ptf9051c)

4. **Update message catalogs and fix message catalog errors in PAM-related code.**

(ID: 531385:2)

5. **Support for remote LDAP server authentication.** --
   A new PAM module (**pam_ldap**)has been added that allows authentication via PAM against an LDAP Server. OpenLDAP has two more files *pam_ldap.so* and *ldap.so* installed as */usr/lib/security/pam_ldap.so* and */usr/lib/nss/ldap.so*. These two files together can be used to provide authentication against an OpenLDAP server.

   (ID: 530735:2 ESC: erg712767)

6. **IBM BladeCenter w/ BIOS 1.09 loops with USB keyboard** --
   This problem has been resolved.
   (ID: 532234:3)

Kernel improvements

1. **Kernel panic in kma_giveback on Maintenance Pack 1** --
   Fixed a kernel panic and possible memory corruption that can occur when a process that has attached shared memory segments fails a fork system call.
   (ID: 530917:1 ESC: erg712782)

2. **Kernel panic in ICH (sound) initialization** --
   ICH Intel Audio driver: If an interrupt comes in during ICH enumeration from a device sharing an IRQ with the AC'97 controller than the *ich_intr*() routine can cause a kernel panic due to incorrect lock allocation during enumeration. This has been fixed.
   (ID: 532377:2)

3. **System upgraded from Release 7.1.2 (8.0.0) experiences kernel panics regularly** --
   Fixed a kernel panic when running LKP binaries, due to a stack corruption.
   (ID: 533255:2)

4. **PCI slot numbers not reported correctly** --
   This problem has been resolved.
   (ID: 533303:2)

5. **TBLNK tunable parameter has incorrect description message** --
   The description for the TBLNK tunable parameter says that the adjustment is in minutes instead of seconds, as it actually is.
   (ID: 530828:2)

6. **Balance callouts across multiple cpus** --
   A problem that could have caused kernel timeouts to bottleneck on cpu 0 has been fixed. Support is added to allow running global callout on any cpu. If this feature is enabled via setting callout_balance to 1 in svc.cf/Space.c, then callouts may execute on cpu other than the boot cpu. This has the affect of running callouts at the precise scheduled time in an heavy system workload.
   (ID: 532367:1 SLS: ptf9051a)

7. **Timeouts for bound drivers may run on wrong cpu** --
   This problem has been fixed.
   (ID: 532326:1 SLS: ptf9051a)

8. **init 0 - unthrottled loop on console input - possible to overheat processor** --
   If after initiating **shutdown**, the system is not powered off after the following message is displayed, the processor heats up:

   ```
   System has halted and may be powered off (Press any key to reboot)
   ```

   Added a spin pause instruction into the loop; this is allegedly thermal friendly.
   (ID: 530708:2 SLS: ptf9051a)

9. **System info defines for SI_SET_VERSION and SI_SET_SYSNAME reuse numbers issued to Solaris** --
   This problem has been resolved.
   (ID: 533077:1)

10. **VxFS snapshot kernel panic using BackupEdge** --
    Fixed 2 kernel panics and a hang related to reading snapshot filesystem via direct I/O.
    (ID: 532771:2)

11. **System hung processes waiting on lock** --
    Asynchronous VxFS transaction log flush can hang forever when MPIO layer detects a path failure and attempts path recovery. This can freeze all other file system activity, and cause system hang. The fix is to setup the correct flags in I/O request buffer when Asynchronous I/O operation is requested.
    (ID: 530400:3 ESC: erg712725)

12. **Kernel panic when running OpenServer binary** --
    This problem has been resolved.
    (ID: 529023:1)

13. **Bad declaration of _h_errno() function return type** --
    Change netdb.vh and libsocket/inet/nd_gethost.c to agree that _h_errno() returns "int *" and not "const int *".
    (ID: 531073:1)

14. **On IBM x445 with 3.0 Ghz cpu(s) the OS does not detect the whole memory after a reboot** --
    Fixed mps and atup psm initialization to do "himem" detection after APIC and PIC initialization or after masking all interrupts on PIC, otherwise unexpected hardware interrupts can cause failure of v86bios() calls to detect "himem" via BIOS e820 interfaces, leading to OS not detecting whole system memory.
    (ID: 530717:2 ESC: erg712765)

15. **Priocntl on an FP-class process running an OpenServer 5 binary may panic the kernel.** --
    For the SVR5 ABI, the value FP_NOCHANGE is defined to be -5. For the OSR5 ABI, this value is SCO_RT_NOCHANGE, defined to be -1. The fix is to have the kernel use FP_NOCHANGE internally to mean "no change", and to have *fp_parmsin* convert SCO_RT_NOCHANGE to FP_NOCHANGE when accepting a request from an OSR5 ABI program.
    (ID: 531493:2)

16. **Kernel panics with trap E after running Java program** --
    This problem has been resolved.
    (ID: 533322:3)

17. **Added new native hot-plug interfaces to SDI so newer drivers can dynamically remove and add targets.**
    (ID: 532894)

18. **PSM fix for Intel S3E31XX (Harwich) BIOS not having BSP as first entry in MPS cpu tbl** --
    The Boot Strap Processor is incorrectly identified on the Intel S3E31xx series (Harwich/Twin Castle) platform. This problem manifests itself as a spontaneous system reset when the remaining processors are brought online. PSM now smarter about location of BSP entry, preventing reboots when additional processors are brought online.
    (ID: 532473:2 SLS: ptf9051)

19. **xAPIC detection is broken on systems with > 8 logical processors** --
    This problem has been resolved.
    (ID: 532824:2 SLS: ptf9051b)

20. **mega driver high CPU consumption** --
    Interrupts may be incorrectly routed when the ACPI boot parameter is set with "ACPI=Y". It may also occur on uniprocessor systems that support hyperthreading and do not have MPS BIOS tables when the ENABLE_JT boot parameter is set with "ENABLE_JT=Y". This problem only manifests itself on systems with complex bus architectures. Symptoms that the fix is required are any of:
    a. High CPU consumption in interrupt time when the system is otherwise idle, as indicated by sar and/or

rtpm.
   b. Devices with interrupt timeouts.
   c. PCI devices that cannot be found.

(ID: 531694:2 SLS: ptf9051a)

21. **ACPI:Unable to access PCI config space error when enabling jt** --
This problem has been fixed.
(ID: 531695:2 SLS: ptf9051)

22. **Deadlock in asyc output stream** --
This problem has been resolved.
(ID: 531720:2 ESC: erg712825)

Security improvements

1. **SECURITY: tcpdump Denial of Service** --
[SCOSA-2005.60] Various flaws in tcpdump can allow remote attackers to cause denial of service. To fix this, tcpdump and libpcap have been updated to version 3.9.3 and 0.9.3 respectively.
(ID: 532314:2 ESC: erg712849)

2. **SECURITY wu-ftp Denial of Service** --
[SCOSA-2005.28] The wu_fnmatch function in wu_fnmatch.c allows remote attackers to cause a denial of service (CPU exhaustion by recursion) via a glob pattern with a large number of * (wildcard) characters, as demonstrated using the dir command.
(ID: 532336:2 ESC: erg712855)

3. **SECURITY: rpcbind Denial of Service** --
[SCOSA-2005.31] When the RPC portmapper (rpcbind) receives an invalid portmap request from a remote (or local) host, it falls into a denial of service state and cannot respond. As a result, the RPC services will not operate normally.
(ID: 532477:2 ESC: erg712862)

4. **SECURITY: telnet client information disclosure** --
[SCOSA-2005.35] The telnet client allows remote malicious telnet servers to read sensitive environment variables via the NEW-ENVIRON option with a SEND ENV_USERVAR command.
(ID: 532338:4 ESC: erg712857)

5. **SECURITY: telnet client multiple issues** --
[SCOSA-2005.21] Buffer overflow in the slc_add_reply function when handling LINEMODE suboptions, allows remote attackers to execute arbitrary code via a reply with a large number of Set Local Character (SLC) commands. Heap-based buffer overflow in the env_opt_add function in telnet.c allows remote attackers to execute arbitrary code via responses that contain a large number of characters that require escaping, which consumers more memory than allocated.
(ID: 531446:2 ESC: erg712801)

6. **SECURITY: uidadmin Buffer Overflow Vulnerability** --
[SCOSA-2005.54] Local exploitation of a buffer overflow vulnerability in the uidadmin binary allows attackers to gain root privileges. Successful exploitation of this vulnerability requires that user have local access to the system. This would allow the user to gain superuser privileges.
(ID: 533178:3)

7. **SECURITY: Racoon Denial of Service** --
[SCOSA-2005.37] Racoon is an IKEv1 keying daemon, a common IPSec Utility. Due to a bug in the way the Racoon parsed incoming ISAKMP packets, an attacker could possibly crash the racoon daemon by sending a specially crafted ISAKMP packet.
(ID: 531604:2 ESC: erg712818)

8. **SECURITY: ICMP TCP connections may be degraded or dropped** --
   [SCOSA-2005.36] The ICMP RFC recommends no security checking for in-bound ICMP messages, so long as a related connection exists, and may potentially allow several different Denials of Service. The following individual attacks are reported: A blind connection-reset attack is reported, which takes advantage of the specification that describes that on receiving a 'hard' ICMP error, the corresponding connection should be aborted. A remote attacker may terminate target TCP connections and deny service for legitimate users. An ICMP Source Quench attack is reported, which exploits the specification that a host must react to ICMP Source Quench messages by slowing transmission on the associated connection. A remote attacker may effectively degrade performance for a legitimate connection. To fix these issues, a new networking parameter tcp_ignore_quench is introduced for configuring ICMP source quench message behavior for tcp connections. When it is set to 1, ICMP source quench messages are ignored for tcp connections. Default value of this parameter is 1.
   (ID: 530661:3 ESC: erg712758)

9. **SECURITY: TCP RFC1323 denial of service** --
   TCP connections can be stalled/dropped using the TimeStamp option of a TCP connection.
   (ID: 531593:2 ESC: erg712814)

10. **SECURITY: ppp prompt buffer overflow vulnerability** --
    [SCOSA-2005.41] Local exploitation of a buffer overflow vulnerability in the ppp binary, allows attackers to gain root privileges.
    (ID: 532994:2 ESC: erg712940)

11. **SECURITY: Xloadimage NIFF Image Title Handling Buffer Overflow** --
    [SCOSA-2005.56] A buffer overflow in xloadimage, might allow user-complicit attackers to execute arbitrary code via a long title name in a NIFF file, which triggers the overflow during (1) zoom, (2) reduce, or (3) rotate operations.
    (ID: 533253:3)

12. **SECURITY: cpio directory traversal vulnerability** --
    [SCOSA-2005.32] A malicious user can create cpio archives containing absolute pathnames and/or relative pathnames like ../ (dot dot/) causing users running cpio -i to inadvertently overwrite files on their system. To prevent it, a new option "-N" is provided for "safe mode", where cpio is trapped inside the present working directory while extracting files.
    (ID: 532333:2 ESC: erg712854)

13. **SECURITY: Lynx Remote Buffer Overflow** --
    [SCOSA-2005.47] A vulnerability in Lynx can be exploited by malicious people to compromise a user's system. The vulnerability is caused due to a boundary error in the "HTrjis()" function in the handling of article headers sent from NNTP (Network News Transfer Protocol) servers. This can be exploited to cause a stack-based buffer overflow by e.g. tricking a user into visiting a malicious web site which redirects to a malicious NNTP server via the "nntp:" URI handler. Successful exploitation allows execution of arbitrary code. As part of this fix lynx has been updated to 2.8.5.
    (ID: 533159:3)

14. **SECURITY: Lynx Command Injection Vulnerability** --
    [SCOSA-2005.55] Remote exploitation of a command injection vulnerability could allow attackers to execute arbitrary commands with the privileges of the underlying user. The problem specifically exists within the feature to execute local cgi-bin programs via the "lynxcgi:" URI handler. The handler is generally intended to be restricted to a specific directory or program(s). However, due to a configuration error on multiple platforms, the default settings allow for arbitrary websites to specify commands to run as the user running Lynx.
    (ID: 533314:3)

15. **SECURITY: libXpm may allow attackers to execute arbitrary code** --
    [SCOSA-2005.57] An integer overflow vulnerability in libXpm can be exploited by a remote user to cause arbitrary code to be executed. The 'scan.c' code does not properly validate user-supplied data contained in image files. A remote user can create a specially crafted image file that, when processed by the target user or application, will trigger the overflow and execute arbitrary code.

(ID: 533161:6)

16. **SECURITY: docview htdig cross site scripting flaw** --
    [SCOSA-2005.45] Cross-site scripting vulnerability in docview (htdig) allows remote attackers to execute arbitrary web script or HTML via the config parameter, which is not properly sanitized before it is displayed in an error message.
    (ID: 531483:2 ESC: erg712807)

Networking improvements

1. **The OpenLDAP Software Suite (openldap) package, version 2.1.22-01:**
    1. **libthread** was not linked properly. The previous configuration used **-lthread** instead of **-Kthread** while building **opendlap**.
       (ID: 530735)

    2. **The binaries are now dynamically linked with LDAP and DB libraries.**
       (ID: 530735)

    3. **Support added for remote LDAP server authentication.** --
       OpenLDAP has two more files *pam_ldap.so* and *ldap.so* installed as */usr/lib/security/pam_ldap.so* and */usr/lib/nss/ldap.so*. These two files together can be used to provide authentication against OpenLDAP server.
       (ID: 530735 ESC: erg712767)

2. **named (9.2.1) fails to switch to secondary forwarder in the event of primary failure** --
   This has been resolved. Additionally, BIND has been updated to version 9.2.5.
   (ID: 532808:3 ESC: erg712896)

3. **telnet sessions have incorrect timestamp in syslog** --
   This problem has been fixed.
   (ID: 532534:1)

4. **netstat command does not find the IP/name of the configured interfaces** --
   netstat was not displaying network and IP addresses properly.
   (ID: 530807:2)

5. **Delays seen when doing rsh, rlogin, or rcp into a UnixWare 714 MP1 box.**
   The pam_rhosts module has been modified to use text-based comparison to check whether the host requesting rsh, rlogin, or rcp is listed in .rhosts or /etc/hosts.equiv. This behavior is consistent with UnixWare behavior in earlier releases which did not support PAM. In contrast, the previous release of the pam_rhosts module used an IP-address comparison to check for host equivalence.
   A new option, "checkaddr," has been added to the pam_rhosts module. Use of this option will cause pam_rhosts to use an IP-address comparison for host equivalance.
   (ID: 530252:2 ESC: erg712708)

6. **To exclude users from password aging rules,** e.g., for FTP, "passwd -n2 -x1 <login>" is used. This is supposed to remove password aging restrictions from the login, so that the password never expires; however, FTP login failures due to password aging still occurred after executing the above. The problem was found in the PAM module for FTP, and has been fixed.
   (ID: 530051:1)

7. **Unloading ipf causes kernel panic** --
   This problem has been resolved in the ipf-4.1.3a package.
   (ID: 531340:2)

8. **Kernel panic in fsflush_pageflush while running du on NFS mount point.** --
   Fixed a race between fsflush which is releasing an un-referenced vnode and NFS rnode allocation code which is trying to re-use the same free'd/inactive vnode, leading to kernel panic.

(ID: 530399:4 ESC: erg712724)

9. **xntpd does not include support for parse clocks like a HOPF6021 clock** --
   Support for HOPF Serial Device and the following clocks is enabled in NTP demon and utilties:

   ```
   o Diem Computime Radio Clock
   o ELV/DCF7000 clock
   o HOPF 6021 clock
   o Meinberg clocks
   o RCC 8000 clock
   o Schmid DCF77 clock
   o WHARTON 400A Series clock
   o VARITEXT clock
   ```

   (ID: 531232:2 ESC: erg712797)

10. **Incompatibility in *bind*() between OSR5 and UW7** --
    OSR5 application socket API compatibility
    (ID: 529470:2)

11. **System hang after pulling NIC cable (e1008g)** --
    This has been resolved. The fix is in the nd-8.0.2c package.
    (ID: 531667:3 ESC: erg712824)

12. **TCP timers can delay other critical activity** --
    On a system with a high TCP connect/disconnect rate (such as a server receiving a large number of web requests), TCP timers such as 2msl, zombie, etc., can take a significant amount of time to process and clean up connections. This has the potential of starving/delaying other non-tcp/tcp timers as well as possibly STREAM activity. This problem has been fixed.
    (ID: 532371:1)

13. **OSR5 ioctl compatibility - TI_GETINFO** --
    OSR5 application ioctl compatibility fix.
    (ID: 533297:3)

14. **MTU is not set correctly in response to an ICMP Error - Fragmentation Needed** --
    This has been resolved.
    (ID: 529427:1 ESC: erg712617)

15. **/etc/mkfilters doesn't generate a valid filter for ipf to use** --
    This problem has been resolved.
    (ID: 532361:2)

16. **DHCP server isn't working** --
    Allow multiple control options to be received.
    (ID: 531979:2)

17. **dlpid does not failover to chain of NICs, nor share backups, mismatching our doc** --
    dlpid updated for failback and failover to chain of NICs.
    (ID: 529245:4)

18. **nfs mount kernel panic if file system exported with anon=-1** --
    If a system exports an nfs file system with anon=-1 and another tries to mount it, the client panics, or the mount command hangs leaving an unkillable process. This problem has been fixed.
    (ID: 531195:2, 531986:2)

19. **e1008g nic driver report same device when network unplugged from 2 different devices** --
    The e1008g driver prints (slot, port) which can be same since the confmgr assigns slot number (0) to all on-board devices and the e1008g driver assigns unique port numbers to devices that have same slot numbers and are on the same bus. If the on-board devices are on different buses, the (slot, port) combination would be same. Modified e1008g driver to print (slot,port,bus) when link goes up/down. The fix is in nd-8.0.2c package.

(ID: 532442:3 ESC: erg712895)

20. **d21x .bcfg files - leading spaces in CUSTOM params screws up ISL.** --
    Removed white space in d21 *.bcfg files as well as mdi_wan - all the .bcfg files for the ISDN code.
    (ID: 530920:1)

USB improvements

1. **Work around problem with IBM Blade Server** (eserver 8677-1xx) BIOS version 1.09 that cause system kernel panic shortly after boot.
   (ID: 531479 SLS: ptf9051a)

2. **USB printing errors on select combinations of printers and write patterns.** --
   Fixed USB printing errors most commonly seen as corruption at end of print job.
   (ID: 532127:2)

3. **Cannot access USB floppy after hot adding and sdiconfig -l output is corrupted** --
   Fixed USB floppy drive issue, non-synchronized assignments of controller number by both pdiunits and SDI layer cause overlapping and conflicting SDI unit numbers asigned to usb_msto, causing problems while accessing USB floppy drive(s).
   (ID: 529971:2 ESC: erg712669)

Motif library and X improvements

1. **The X11R6 X Server (xserver) package, version 8.0.2c:**
    1. **SECURITY: Xserver local users can gain root** --
       [SCOSA-2004.2] Buffer overflow in the ReadFontAlias function in Xsco may allow local or remote authenticated users to execute arbitrary code via a malformed entry in the font alias file.
       (ID: 528865:2 ESC: erg712546)/OS/Gui/X_Motif/XSrvr

    2. **A memory corruption in the X server was causing the X server to crash.** --
       This problem has been resolved.
       (ID: 530745 ESC: erg712769)

    3. **The X server does not properly display a dotted line separator.** --
       This problem has been resolved.
       (ID: 531054:2 ESC: erg712794)

2. **X clients receive FocusIn event twice**, first when the window is clicked and second when a widget a clicked. This problem has been resolved.
   (ID: 531053:2 ESC: erg712793)

3. **A black mark is displayed under the first character** if the height of a text widget is smaller than the height of the character. This problem has been resolved.
   (ID: 532175:2 ESC: erg712839)

4. **Problem with list items in list widgets fixed.** If a user clicks on an item in a List widget with SelectionPolicy set to BROWSE_SELECT or SINGLE_SELECT and then clicks on another list item within DoubleClickInterval, the click is treated as second click of the double-click on the original item. The visual affect is that the cursor moves to the second item while the highlight frame remains on the first one. The problem is not seen with short DoubleClickInterval because it's very difficult to do the second click on a different item within that short interval.
   (ID: 532813:2 ESC: erg712897)

5. **A dotted line separator is not displayed correctly.** --
   This problem has been resolved.
   (ID: 531054:2 ESC: erg712794)

6. **Focus is not set on newly created windows in mwm** --
   The Motif window manager sometimes does not set focus on the newly created windows. This problem has been resolved.
   (ID: 533334:2)

7. **In the Japanese keyboard input environment, the Xserver dies after certain keyboard operations.** --
   Optimized code in the server was causing memory corruption in these circumstances. The calls to optimized functions were replaced with calls to unoptimized functions, and the problem has been resolved.
   (ID: 530745:2 ESC: erg712769)

8. **Support for ATI Radeon ES1000/RN50 graphics card** --
   Support for the ES1000/RN50 video card has been added to the xdrivers-8.0.2b package.
   (ID: 532713:1)

9. **Permission of *`/usr/X/lib/X11/xkb/symbols`* directory is 0644** --
   This causes incorrect LED behavior on the keyboard. Permissions on the directory */usr/X/lib/X11/xkb/symbols* changed to 0755.
   (ID: 528560:3)

Commands

1. **The more command does not properly handle files with multibyte characters.** It splits multibyte characters across lines and gives the following error:

   ```
   more: Illegal byte sequence
   ```

   (ID: 531424 ESC: erg712800)

2. **The file command and *`/etc/magic`* file have been enhanced** to provide better and POSIX compliant reporting of command text file types, additional information about ELF object files and core dumps, and recognize additional special file types.
   (ID: 532351)

3. **The cm_vtcld and scoadmin utilities core dump when SFNOLIM is tuned higher than 32767.**
   (ID: 527772:3 ESC: erg712304)

4. **After using `ap`, owner accounts can't gain owner privs** --
   Fixed the failure to get owner privileges when logged in as owner.
   (ID: 533134:2 ESC: erg712965)

5. **Can't display multibyte character on samba-3.0.4** --
   The **iconv** command failed to convert between the eucJP and sjis codesets with the following error message:

   ```
   UX:iconv: ERROR: No support for eucJP to sjis
   ```

   This problem has been resolved.
   (ID: 530767:2 ESC: erg712771)

6. **Further tapecntl commands blocked after tapecntl -e interrupted** --
   Added support for tape erase i/o process abort in tapecntl and st01.
   (ID: 529485:3 ESC: erg712616)

7. **Mailx - incorrect optimiztion in collect.c - stripnulls()** --
   Updated */usr/bin/mailx.*
   (ID: 531705:3)

8. **fdisk formatting needs update for large disks (> 10K cyls / 76.6 GB)** --
   Increased **fdisk** column widths for larger disk sizes, to prevent column overrun/staircase display for multiple partitions.
   (ID: 530772:2)

Development System

The fixes in this section are contained in the **uw714m3**, **libc**, and **uccs** packages.

1. **Segementation faults fixed.** Repaired bugs which, in certain situations involving extra long lines in the */etc/passwd*, */etc/group*, or */etc/shadow* files, caused stale pointers to be dereferenced, likely resulting in segmentation faults.
   (ID: 531950 ESC: erg712834)

2. **Add support for classic OpenServer "gencat" message catalogs.**
   (ID: 532671)

3. **Move the *getmnt*, putmntent, getvfs**, putvfsent APIs from *libgen* into the shared part of the C library.**
   (ID: 531331)

4. **Add the *setenv*() and *unsetenv*() APIs (matching The Open Group specifications) to the C library.** --
   The routines have been added.
   (ID: 533075:1)

5. **The cc command now supports compiling *.S*-suffixed files.** --
   These are assembly language source files that are first passed through the C preprocessor. This allows for assembly language coding across different assembler dialects. The **cc** command has been modified to support .S files. They are sent to the usual **acpp** preprocessor, with an additional option to request no extra whitespace insertion. Note that support for *.S* was *not* added to the **CC** command, since the additional complexity required to support it in **CC** is not justified by the modest user benefit it would provide.
   (ID: 531455:6, 531445:7)

6. **Copy propagation optimizations may have failed to consider side-effects in the left operand of an assignment statement,** resulting in incorrect code being generated for statements of the form:

   ```
   *ptr1++ = .... *ptr2 ....
   ```

   and both pointers had the same value an earlier sequence point in the current code block.
   (ID: 531705)

7. **The C (C++) compiler support for *_Bool* (*bool*) was corrected so that all arithmetic operations will store either a 0 or 1 to a boolean object.**
   (ID: 531941, 532751)

8. **The C compiler support for compound literals was corrected so that they are appropriately reinitialized when used as part of a loop's controlling expression.**
   (ID: 531447, 531350)

9. **The C and C++ compiler floating expression evaluation will now correctly narrow (by default and with -Kieee) the value which results from a floating-typed assign-op computation.**
   (ID: 531447, 531350)

10. **The redundant push/pop elimination optimization** done by the assembly peep-hole optimizer (**optim**) may have incorrectly used the EAX scratch register when it holds the function return value obtained from a call to another function.
    (ID: 532298)

11. **Plum Hall CV suite (cvs04a) - multiple issues** --
    This problem has been resolved.
    (ID: 531249:2)

12. **Automatic compound literal initialization repeated in loop - PH conform/lang** --
    This problem has been resolved.
    (ID: 531250:2)

13. **strip/mcs fail to adjust section indices for newer ELF features** --
    Change strip/mcs code to adjust these additional section indices. Note that this is the only instance where strip/mcs will fiddle with the contents of a section. Also need to update the ELF headers to have the missing SHT_ and SHF_ macros.
    (ID: 533355:1)

14. **Copy propagation does not check for side-effect on left side of tree** --
    This has been resolved.
    (ID: 531705:4)

15. **Inconsistant rounding in CSE temp** --
    This changes floating point code generation for C and C++ in those circumstances where a floating "common subexpression" is saved for later use. Instead of saving it with the precision of its implicit type, it will be saved as a full- width 80-bit value so that when it is later used it behaves just as if it had been recomputed for each such use.
    (ID: 532927:1)

16. **optim is trying to keep both halves of a 64 bit value in 1 32 bit register** --
    Update a function within optim to check whether registers contain implicitly live data before using them.
    (ID: 532298:2)

17. **Optim generates some incorrect code following boolean fixes.** --
    This problem has been resolved.
    (ID: 531941:2)

18. **Order of object files in lib++.a inconsistent from build to build** --
    Change made as suggested in incident.
    (ID: 532693:1)

19. **getXXent_r() APIs misbehave when the buffer is too short** --
    Add code to reset to the start of the line in this situation for the C library APIs. For the NIS aware ones, have it reuse the already created struct in this case.
    (ID: 533169:1)

20. **Two bugs in getgr* and getpw*** --
    Just need to include the NIS_SCAN bit when setting the NIS_FIRST one for the nss_nis_get*ent*() routines.
    (ID: 530952:3)

21. **/usr/include/net/if.h compile errors in C++** --
    This problem has been fixed.
    (ID: 531548:2)

Application Fixes

- **The Open Secure Shell (openssh) package, version 4.2p1:**
  1. **SECURITY: OpenSSH has been updated from version 3.9p1 to 4.2p1.** --
     [SCOSA-2005.53] Please see the openssh website for the list of changes. http://www.openssh.com/
     (ID: 532373:1, 532978 ESC: erg712922, erg712933)

- **cdrtools - A set of tools for CD/DVD Recorders package, version 2.01.01a01:**
  1. SECURITY: [SCOSA-2005.20] Cdrtools has been updated from version 2.01a27 to 2.01.01a01 to fix the following problem:
     Cdrecord in the cdrtools package before 2.01, when installed setuid root, does not properly drop privileges before executing a program specified in the RSH environment variable, which allows local users to gain privileges.

     (ID: 530156:2 ESC: erg712690)

- **The ESP Ghostscript (gs) package, version 7.07.1:**
  1. ESP Ghostscript has been updated from version 7.05.6 to 7.07.1. Please see the cups website for the list of changes. http://www.cups.com/
     (ID: 532587:1)

- **The GNU file compression utilities (gzip) package, version 1.3.5:**
  1. **SECURITY: Gzip Multiple Vulnerabilities**
     [SCOSA-2005.58] gzip crashes when an input file name is longer than 1020 characters.

     zgrep in gzip does not properly sanitize arguments, which allows local users to execute arbitrary commands via filenames that are injected into a sed script.

     Race condition in gzip, when decompressing a gzipped file, allows local users to modify permissions of arbitrary files via a hard link attack on a file while it is being decompressed, whose permissions are changed by gzip after the decompression is complete.

     Directory traversal vulnerability in gunzip -N allows remote attackers to write to arbitrary directories via a .. (dot dot) in the original filename within a compressed file.
     (ID: 532919:2 ESC: erg712915)

  2. **Gzip updated to handle large files (<4GB).**
     (ID: 532327 ESC: erg712850)

- **The Squid Caching Proxy Server (squid) package, version 2.5.STABLE12:**
  1. **SECURITY: [SCOSA-2005.44] Squid has been updated from version 2.5.STABLE7 to 2.5.STABLE12 to fix several security problems.** --
     Please see the squid website for the list of changes. http://www.squid-cache.org/
     (ID: 530961, 530961, 533116, 533151, 533254 ESC: erg712785, erg712785)

  2. **Reinstated the following which were inadvertently dropped when squid was updated to 2.5.STABLE7:**

     ```
     o CARP
     o Heap removal policy
     o ICMP
     o Delay pools
     o User-Agent logging
     o Kill parent on shutdown
     o SNMP monitoring
     o HTCP
     o USE_CACHE_DIGESTS
     ```

     Additionally enabled the following:

     ```
     o Referer logging
     ```

     (ID: 531636:2 ESC: erg712823)

- **The TIFF Library and Utilities (tiff) package, version 3.7.3:**
  1. **SECURITY: [SCOSA-2005.19 SCOSA-2005.34] Tiff has been updated from version 3.5.7 to 3.7.3 to fix several security problems.** Please see the tiff website for the list of changes.
     http://www.remotesensing.org/libtiff/
     (ID: 531015, 532775 ESC: erg712790, erg712889)

- **The MySQL package - multi-threaded SQL database server (MySQL), version 4.1.11:**
  1. **SECURITY: [SCOSA-2005.27] MySQL has been updated from 3.23.49 to 4.1.11 to fix security problems.** --
     Please see MySQL website for the list of changes.
     (ID: 531603 ESC: erg712817)

- **The Mozilla (mozilla) package, version 1.7.12:**

Note: After installing the latest Mozilla package, you will also need to download and install the latest Java packages so that Mozilla continues to work properly. The Java packages are available separately from the UnixWare 7.1.4 Supplement Page at:
http://www.sco.com/support/update/download/product.php?pfid=1&prid=6.

1. **SECURITY: [SCOSA-2005.25] [SCOSA-2005.29] Mozilla has been updated from 1.2.1b to 1.7.12 to fix several security problems.** --
   Please see the Mozilla website for the list of changes.
   (ID: 528733:2, 528734:2, 530151:2, 530485:2, 530642:2, 531626:2, 532631:2, 532645:2, 533017:1 ESC: erg712686, erg712734, erg712748, erg712820)

Other Fixes

1. **The Berkeley DB Library (db) package, version 4.1.25:**
   1. Minor configuration changes were done while building the db library.
      (ID: 530735)

   2. The Documentation was moved from */usr/docs* to */usr/share/db/doc/* and link was added to DocView.
      (ID: 530735)

2. **The General Purpose Data Compression Library (zlib) package, version 1.2.3:**
   1. **SECURITY: [SCOSA-2005.33] zlib has been updated from version 1.2.1-01 to 1.2.3 to fix several security problems.** --
      Please see the zlib website for the list of changes. http://www.zlib.net
      (ID: 532198:1, 532826 ESC: erg712898)

3. **The OpenSSL (openssl) package, version 0.9.7i:**
   1. **SECURITY: OpenSSL has been updated from version 0.9.7d to 0.9.7i.** --
      [SCOSA-2005.48] Please see the openssl website for the list of changes. http://www.openssl.org/
      (ID: 531858:1, 533160)

   2. **The OpenSSL Documentation (openssld) package,** version 0.9.7i, provides the updated documentation for the openssl package version 0.9.7i.

4. **UW7.1.4 ide driver returns Undefined Symbol fs_clrioevent in loadable module** --
   While prototyping, doGetHBA has been changed to force the user to first load the HBA's from the base OS CD and then give the options to load the TP HBAs. This ensures that the .extra.d/ tools are also copied properly.
   (ID: 530541:1 ESC: erg712766)

5. **URK714:Filesystem missing from vfstab is not replicated** --
   sliceinfo script has been changed to mount the slices having fs but not mounted to temporary mount points and hence replicated properly.
   (ID: 530568:1 ESC: erg712744)

6. **Listing groups using the ScoAdmin Account Manager dumps core for certain sized group entries** --
   Long entries in */etc/passwd*, */etc/group*, and */etc/shadow* caused the *listgrp* function to dump core. This has been fixed.
   (ID: 531950:2 ESC: erg712834)

7. **Provide updated MySQL package for UnixWare 7.1.4 MP CD** --
   MySQL package now included in ISO image.
   (ID: 530657:1)

8. **SCO Clusters license definitions** --
   Added SCO Clusters licenses in the default product database.
   (ID: 533284:2)

9. **Need PMAPI calls for user and cpu counts** --
   This problem has been resolved.

(ID: 532928:2)

Drivers

1. **Intel e1008g Gigabit driver 2.7.5 reports "Speed/Dx:10/H"** --
   This problem has been resolved.
   (ID: 517482:1)

2. **Intel Centrino Wireless driver** --
   ipw, Intel Centrino PRO/Wireless 2200BG NIC driver supported adapters: Intel PRO/Wireless 2200BG NIC (built in laptop)
   (ID: 531382:2)

3. **Intel PRO/100 eeE8 version 3.0.2 driver** --

```
eeE8 3.0.2, Intel(R) PRO/100 supported adapters:

================== CardBus Adapters ============

 Intel PRO/100 CardBus II        MBLA3300
 Intel PRO/100 S Mobile Adapter  MBLA3300 C3
 Intel PRO/100 CardBus II        MBLA3400

 645477-xxx    PRO/10+ PCI                              PILA8500
 649439-xxx    PRO/10+ PCI                              PILA8520
 701738-xxx    Pro/100+ PCI Management Adapter          PILA8461
 668081-xxx    Pro/100+ PCI                             PILA8460

 721383-xxx    Pro/100+ PCI Management Adapter          PILA8460B
 741462-xxx    Pro/100+ PCI                             PILA8460BN
 748566-xxx    PRO/100 S Management                     PILA8460BUS
 748564-xxx    PRO/100 S Management                     PILA8464B
 742252-xxx    InBusiness(tm) 10/100 adapter            SA101TX
 351361-xxx    PRO/100 PCI                              PILA8465
 352509-xxx    EtherExpress(tm) PRO/100B PCI adapter    PILA8465B

 352433-xxx    PRO/100B PCI T4                          PILA8475B
 691334-xxx    PRO/100+ PCI Management  Adapter         PILA8900
 A80897-xxx    PRO/100 M Desktop                        PILA8460M
 751767-xxx    PRO/100 S Desktop                        PILA8460C3

 ================== Server Adapters ============

 714303-xxx   PRO/100+ Dual Port Server Adapter         PILA8472
 748565-xxx   PRO/100 S Server                         PILA8474B
 748568-xxx   Intel(c)PRO/100 S Server                 PILA8474BUS
 710550-xxx   PRO/100+ PCI Server Adapter              PILA8470
 729757-xxx   PRO/100+ Server Adapter                  PILA8470B
 A56831-xxx   PRO/100 S Dual Port Server Adapter       PILA8472C3
 752438-xxx   PRO/100 S Server                         PILA8470C3
 A28276-001   Intel(c) PRO/100+ Dual Port Server Adapter 61PMCA00

 82559 Fast Ethernet LOM with Alert on LAN
 PRO/100 S Mobile LAN on Motherboard

 PRO/100 VM Network Connection
 PRO/100 VE Network Connection

 HP NC1120 Ethernet NIC
 HP NC3120 Fast Ethernet NIC
 HP NC3121 Fast Ethernet NIC
 HP NC3122 Fast Ethernet NIC
 HP NC3123 Fast Ethernet NIC
 HP NC3131 Fast Ethernet NIC
 HP NC3132 Fast Ethernet NIC
 HP NC3133 Fast Ethernet NIC
 HP NC3134 Fast Ethernet NIC
 HP NC3135 Fast Ethernet Upgrade Module
 HP NC3160 Fast Ethernet NIC
 HP NC3162 Fast Ethernet NIC
 HP NC3163 Fast Ethernet NIC
 HP 10/100 TX PCI Intel WOL UTP Controller
```

(ID: 532544:1)

4. **Kernel panic during reboot in closef_l+83 -> spec_close+200 -> device_close+43.** --
Race condition in DLPI open and close causing memory corruption.
(ID: 532230:2)

5. **nics and nd packaging rework** --
The *tcpdump* binary, and the *libpcap* library and header files have been moved from the **nd** package to the **nics** package.
(ID: 533124:2)

VII. Maintenance Pack Notes and Limitations

1. After installing the updated **nd** package, you may see the following warning message on every boot:

   ```
   WARNING: eeE8: eeE8ValidateChecksum: EEPROM checksum validation failed
            (slot5,port1)
   ```

   This warning comes from the eeE8 driver version 3.0.2 for the following NIC:

   Vendor ID 0x8086 (INTEL)
   Device ID 0x1229
   Subsystem Vendor ID 0x8086
   Subsystem ID 0x9

   This message can be safely ignored.
   (ID: 530830)

2. Due to changes in the PC Card subsystem, if you have a Network Interface Card (NIC) configured in your laptop prior to installing this maintenance pack, it will not function after the MP is installed. To enable it, you must run the Network Configuration Manager (**scoadmin network** or **netcfg**), remove the NIC, and then add it again.

3. Before you can configure a PC Card NIC in your laptop, the **pcic** driver must be configured using the following steps:

   1. Power down the laptop.
   2. Insert your PC Card NIC into a slot.
   3. Power on the system. On Toshiba laptops, enter the system BIOS as the system comes up and ensure that the following parameter is set as shown:

      Controller Mode = Cardbus/16-bit

   4. Log in as *root*.
   5. Run the Device Configuration Utility: 'dcu'.
   6. Select 'Software Device Drivers'.
   7. Select 'Miscellaneous'.
   8. Page down to the 'pcic' driver.

      If the **pcic** driver is already marked by an asterisk (*), then the driver is already configured. Exit the **dcu** without saving your changes and skip to Step 17.

      Otherwise, select the 'pcic' driver using the space bar.

   9. Press **F5** (New).
   10. Set the following values:

       ```
       Unit:     0
       IPL:      0
       ITYPE:    0
       IRQ:      0
       IOStart:  0
       IOEnd:    0
       MemStart: This field is automatically set by the pcic driver.
                 Don't change this setting.
       MemEnd:   This field is automatically set by the pcic driver.
                 Don't change this setting.
       DMA:      -1
       ```

```
BindCPU:  Leave this field blank.
```

11. Press F10 (Apply and Return).
12. Press Enter (Return).
13. Select 'Return to DCU Main Menu'.
14. Select 'Apply Changes and Exit DCU'.
15. At the *root* prompt, enter the following three commands:

```
# rm /etc/conf/pack.d/pcic/_drv.o
# /etc/conf/bin/idbuild -B
# init 6
```

16. When the system is booting up, you should see a message indicating that the card was detected following the copyright screen. For example:

```
EG: Intel Pro/100 Cardbus PC Card detected in socket 0
```

17. Run the Network Configuration Manager (**scoadmin network** or **netcfg**) to configure your NIC.
18. Exit the Network Configuration Manager and reboot:

```
init 6
```

4. If you are running the OpenServer Kernel Personality (OKP), you may see error messages like the following after installing the MP:

```
UX:unixware: ERROR: Unable to change root to /unixware: Invalid argument
```

This is caused by the default setting of the new CHROOT_SECURITY parameter (see #8 in "Problems Fixed in Maintenance Pack 2", above). In order for OKP to function properly, you must set CHROOT_SECURITY to "0" and reboot the system.
(ID: 531761)

VIII. Copyrights

The following Copyright Notice is required by the **lsof** command source:

```
/*
 * Copyright 2002 Purdue Research Foundation, West Lafayette,
 * Indiana 47907.  All rights reserved.
 *
 * Written by Victor A. Abell
 *
 * This software is not subject to any license of the American
 * Telephone and Telegraph Company or the Regents of the
 * University of California.
 *
 * Permission is granted to anyone to use this software for
 * any purpose on any computer system, and to alter it and
 * redistribute it freely, subject to the following
 * restrictions:
 *
 * 1. Neither the authors nor Purdue University are responsible
 *    for any consequences of the use of this software.
 *
 * 2. The origin of this software must not be misrepresented,
 *    either by explicit claim or by omission.  Credit to the
 *    authors and Purdue University must appear in documentation
 *    and sources.
 *
```

```
 * 3. Altered versions must be plainly marked as such, and must
 *    not be misrepresented as being the original software.
 *
 * 4. This notice may not be removed or altered.
 */
```

Document Issued: December 2005