# Tru64 UNIX Version 5.0

## Patch Summary and Release Notes for Patch Kit-0003

**February 2001**

This manual contains the release notes and describes the contents of Patch Kit-0003. It provides any special instructions for installing individual patches.

For information about installing or removing patches, baselining, and general patch management, see the *Patch Kit Installation Instructions*.

**Compaq Computer Corporation**
**Houston, Texas**

# Contents

# About This Manual

This manual contains information specific to Patch Kit-0003 for the Tru64 UNIX Version 5.0 operating system. It provides a list of the patches contained in each kit and provides any information for installing specific patches.

For information about installing or removing patches, baselining, and general patch management, see the *Patch Kit Installation Instructions*.

## Audience

This manual is for the person who installs and removes the patch kit and for anyone who manages patches after they are installed.

## Organization

This manual is organized as follows:

*Chapter 1* Contains the release notes for this patch kit.

*Chapter 2* Summarizes the base operating system patches included in the kit.

## Related Documentation

In addition to this manual, you should be familiar with the concepts and mechanisms described in the following Tru64 UNIX documents:

- Tru64 UNIX *Patch Kit Installation Instructions*
- Tru64 UNIX *Installation Guide*
- Tru64 UNIX *System Administration*
- Any release-specific installation documentation

## Reader's Comments

Compaq welcomes any comments and suggestions you have on this and other Tru64 UNIX manuals.

You can send your comments in the following ways:

- Fax: 603-884-0120 Attn: UBPG Publications, ZK03-3/Y32
- Internet electronic mail: `readers_comment@zk3.dec.com`

  A Reader's Comment form is located on your system in the following location:

  `/usr/doc/readers_comment.txt`

- Mail:

  Compaq Computer Corporation
  UBPG Publications Manager
  ZK03-3/Y32
  110 Spit Brook Road
  Nashua, NH 03062-9987

Please include the following information along with your comments:

- The full title of this document.
- The section numbers and page numbers of the information on which you are commenting.

- The version of Tru64 UNIX that you are using.
- If known, the type of processor that is running the Tru64 UNIX software.

The Tru64 UNIX Publications group cannot respond to system problems or technical support inquiries. Please address technical questions to your local system vendor or to the appropriate Compaq technical support office. Information provided with the software media explains how to send problem reports to Compaq.

# 1

# Release Notes

This chapter provides information that you must be aware of when working with Tru64 UNIX Version 5.0 Patch Kit-0003.

## 1.1 Required Storage Space

The following storage space is required to successfully install this patch kit:

**Base Operating System**

- Temporary Storage Space

  A total of ~250 MB of storage space is required to untar this patch kit. It is recommended that this kit not be placed in the /, /usr, or /var file systems because this may unduly constrain the available storage space for the patching activity.

- Permanent Storage Space

  Up to ~39 MB of storage space in /var/adm/patch/backup may be required for archived original files if you choose to install and revert all patches. See the *Patch Kit Installation Instructions* for more information.

  Up to ~40 MB of storage space in /var/adm/patch may be required for original files if you choose to install and revert all patches. See *Patch Kit Installation Instructions* for more information.

  Up to ~542 KB of storage space is required in /var/adm/patch/doc for patch abstract and README documentation.

  A total of ~152 KB of storage space is needed in /usr/sbin/dupatch for the patch management utility.

## 1.2 New dupatch Features

Beginning with Revision 26–02 of dupatch, this patch tool utility has been enhanced to provide new features, as described in the following sections. For more information, see the *Patch Kit Installation Instructions*.

### 1.2.1 Patch Installation from Multiuser Mode

Patches can now be installed when a system is in multiuser mode.

There are no restrictions on performing patch selection and preinstallation checking in multiuser mode.

However, although you can now install patches in multiuser mode, Compaq recommends that you bring down your system to single-user mode when installing patches that affect the operation of the Tru64 UNIX operating system (or the product you are patching). If your system must remain in multiuser mode, it is recommended that you apply the patches when the system is as lightly loaded as possible.

### 1.2.2 Patch Installation from a Pseudo-Terminal

Patches can now be installed on the system from a pseudo-terminal (pty) while in single-user mode. To do this, log into the system as root from a remote location and

specify that the patches are to be installed in single-user mode. Once all the patch prerequisites are completed, the system will be taken to single-user mode while maintaining the network connection for the root user. The patches will then be installed by the system.

### 1.2.3 Automatic Kernel Build

If the patches installed indicate that a kernel build is required, `dupatch` will initiate the kernel build automatically.

Most times a reboot is required to complete the installation and bring the system to a consistent running environment. Certain file types, such as libraries, are not moved into place until you reboot the system.

When installing patches in multiuser mode, you can take one of three options after the kernel build is complete:

- Reboot the system immediately.
- Reboot the system at a specified time.
- Forgo a system reboot.

## 1.3 Release Note for dupatch

When you are installing the patch kit you may see a message similar to the following::

```
=== Installing "Tru64 UNIX V5.0" Patches:

/usr/sbin/dupatch:  //usr/sbin/setld:  not found
```

If you see this message, halt `dupatch` and restart the installation. The prior operation did not affect your system in any way, and `dupatch` should now operate properly.

## 1.4 Release Note for dsfmgr

After installing this patch kit, the following error may be displayed during reboot:

```
dsfmgr: ERROR: file "/etc/dfsl.dat" : No such file or directory
bcheckrc: Device Naming failed boot configure or verify.
  Please correct the problem and continue or reboot

INIT: SINGLE-USER MODE
#
```

This error message is benign. There is a small time period when `dsfs*` files may not be available during an update. You may ignore the message and continue the boot at the single user prompt.

## 1.5 Release Note for Patch 225.00

### 1.5.1 UFS throttle mount Option

A new `mount` option, `throttle`, has been added in this patch. To activate this new option, update your `/etc/fstab` entries to enable the selected `mount` option (`throttle`) on the selected UFS filesystems.

For example, change from:

```
/dev/disk/dsk12e /mnt/test ufs rw 0 2
```

to:

```
/dev/disk/dsk12e /mnt/test ufs rw,throttle 0 2
```

Append to/etc/sysconfigtab any tuning changes. Refer to the Tuning notes that follow for a description of the new io-throttle-shift and io-throttle-maxmzthruput tunables. These tunables are configured in the vfs stanza. The following three lines make up an example:

```
vfs:
    io-throttle-shift = 1
    io-throttle-maxmzthruput = 1
```

**Note**

If you already have a vfs stanza in your sysconfigtab file, then just add the two io-throttle entries.

When removing this patch, be sure to remove any additions to /etc/fstab you may have made (see previous instructions).

Failure to remove /etc/fstab modifications may result in unknown attribute messages, particularly upon system reboot.

### Tuning

The purpose of this patch is to minimize system stalls resulting from a heavy system I/O load.

I/O throttling addresses the concern of locking dirty pages on the device queue. It enforces a limit on the number of delayed I/O requests allowed to be on the device queue at any point in time. This allows the system to be more responsive to any synchronous requests added to the device queue, such as a read or the loading of a new program into memory. This may decrease the duration of process stalls for specific dirty buffers, as pages remain available until placed on the device queue.

The relevant tunable variables are as follows:

io-throttle-shift

The greater the number of requests on an I/O device queue, the longer the time required to process those requests and make those pages and device available. The number of concurrent delayed I/O requests on an I/O device queue can be throttled by setting the io-throttle-shift tunable. The throttle value is based on this tunable and the calculated I/O completion rate. The throttle value is proportional to the time required to process the I/O device queue.

The correspondences between io-throttle-shift values and the time to process the device queue areas follows:

| io-throttle-shift | time to process device queue (sec) |
|---|---|
| -2 | 0.25 |
| -1 | 0.5 |
| 0 | 1 |
| 1 | 2 |
| 2 | 4 |

For example, an io-throttle-shift value of 0 corresponds to accommodating 1 second of I/O requests. The valid range for this tunable is [-4..4] (not all values are shown in the above table; you can extrapolate). The default value of io-throttle-shift is 1. Environments particularly sensitive to delays in accessing the I/O device might consider reducing the io-throttle-shift value.

io-maxmzthruput

This is a toggle which trades off maximizing I/O throughput against maximizing the availability of dirty pages. Maximizing I/O throughput works more aggressively to keep the device busy, but within the constraints of the throttle. Maximizing the

availability of dirty pages is more aggressive at decreasing stall time experienced when waiting for dirty pages.

The environment in which you might consider setting `io-maxmzthruput` to off (0) is one in which I/O is confined to a small number of I/O intensive applications, such that access to a specific set of pages becomes more important for overall performance than does keeping the I/O device busy. The default value of `io-maxmzthruput` is 1. Environments particularly sensitive to delays in accessing sets of frequently used dirty pages might consider setting `io-maxmzthruput` to 0.

`io-throttle-static`

If nonzero, the device queue limit is set to this value and it is not dynamically altered.

### 1.5.2 UFS delayed mount Option

This new `mount` option, `delayed`, allows for disabling synchronous metadata writes on a specified filesystem.

To maintain the file system's consistency, UFS metadata (such as inode, directory, and indirect blocks) is updated synchronously by default.

Metadata updates are typically performed synchronously to prevent filesystem corruption after a crash. The trade-off for this filesystem integrity, however, is performance. In some cases, such as a filesystem serving as a cache, performance (faster metadata update) is more important than preserving data consistency across a system crash; for example, files under `/tmp` or web proxy servers such as Squid.

This means two things. One is that multiple updates to one block becomes only one block write, as opposed to multiple writes of the same block with traditional synchronous metadata update. The other is that users can experience much better responsiveness when they run metadata intensive applications because metadata writes will not go out to the disk immediately while users get their prompt back as soon as the metadata updates are queued.

This `delayed` option should not be used on the `/` or `/usr` filesystems. It should be used only on filesystems that do not need to survive across a system crash.

To enable the `delayed` option, run:

**`mount -o delayed`**

or

**`mount -u -o delayed mount -u -o delayed`**

## 1.6 Release Note for Patch 25.00

This patch removes a Granularity Hint Regions (also called GH chunks) restriction which may be encountered on AlphaServer DS20 and ES40 systems running the Tru64 UNIX 5.0 release. This restriction can reduce performance for certain data base applications.

The following error message on the system's console terminal (also logged in `/var/adm/messages`) indicates possible performance loss for applications using GH chunks:

`gh_chunks value of # invalid`

where # is a number which varies depending on memory size.

To remove the GH chunks restriction you need to modify your target kernel configuration file (and rebuild the kernel) and change the state of a console

firmware environment variable. Use the following procedure to make these changes:

1. Follow the steps the *Guide to System Adminstration*, with the following exceptions:

   In step 4, edit the configuration file and add the following line:

   ```
   makeoptions LOADADDR="fffffc0000430000"
   ```

   just before the first line starting with `makeoptions`.

   In step 6, instead of `/usr/sbin/shutdown -r now`, add the following:

   ```
   /usr/sbin/shutdown -h now
   ```

2. Check the console firmware version:

   ```
   P00>>>show version
   ```

   If the version is not V5.5 or later, you need to upgrade your firmware to V5.5 or later.

3. Change the value of the console_memory_allocation environment variable from `old` to `new` and reset the system:

   ```
   P00>>>set console_memory_allocation new
   P00>>>init
   ```

4. Boot the new kernel:

   ```
   P00>>>boot
   ```

   In the unlikely event the new kernel fails to boot:

   ```
   P00>>>set console_memory_allocation old
   P00>>>init
   P00>>>boot -fi vmunix.save
   ```

   or:

   ```
   P00>>>boot -fi genvmunix
   ```

   Correct the error and repeat the above procedure.

### Additional Information

- If you encounter the following error message, you have most likely attempted to boot a kernel with the old load address:

  ```
  Bootstrap address collision, image loading aborted
  ```

  To boot old kernels:

  ```
  P00>>>set console_memory_allocation old
  P00>>>init
  P00>>>boot
  ```

  **Note**

  The generic kernel (`/genvmunix`) will boot with `console_memory_allocation` set to old or new.

- The patch kit installs a new `/usr/sbin/sizer` command. If you rebuild the kernel using section 4.5.1 or 4.5.2 of the *Guide to System Administration*, the new sizer will automatically adjust the kernel's load address.

**Note**

If you customized your existing configuration file, `doconfig` allows you to edit the new configuration file so you can restore your customizations.

## 1.7 Release Note for Patch 282.00

This patch provides additional information for Patch 282.00.

### 1.7.1 PCI To Ethernet/Graphics Combo Adapter (3X-DEPVD-AA)

This patch provides the driver support for the PCI To Ethernet/Graphics Combo Adapter (3X-DEPVD-AA) (also known as the ITI6021E Fast Ethernet NIC 3D Video Combination Adapter, InterServer Combo, or JIB). In order to obtain full support for the PCI To Ethernet/Graphics Combo Adapter (3X-DEPVD-AA), you must also select Patch 58.00, which is the X server portion of the patch.

If you have a system with this adapter, you will need to reconfigure and rebuild the kernel after installing this patch. To do this, follow these steps:

1. Shut down the system:

   # **/usr/sbin/shutdown -h now**

2. Boot genvmunix to single-user mode:

   >>> **boot -fi genvmunix -fl s**

3. After the system boots to single-user mode, mount the file systems, run the `update` command, and activate the swap partition:

   # **sbin/bcheckrc**

   # **/sbin/update**

   # **/sbin/swapon -a**

4. Run `doconfig` to create a new kernel configuration file and rebuild the kernel:

   # **# /usr/sbin/doconfig**

   **Note**

   Do not specify the `-c` option to `doconfig`. If you do, `doconfig` will use the existing kernel configuration file which will not have the appropriate controller entry for the PCI To Ethernet/Graphics Combo Adapter.

5. Save the old `/vmunix` file and move the new kernel to `/vmunix`.

6. Shut down the system:

   # **/usr/sbin/shutdown -h now**

7. Boot the new kernel:

   >>> **boot**

If you remove this patch from your system after you have rebuilt the kernel to incorporate support for the PCI To Ethernet/Graphics Combo Adapter as described previously, you will need to rebuild the kernel again to restore generic VGA graphics support. To do this, follow the steps described previously.

If you run `doconfig` on the original, unpatched genvmunix, it will not recognize the PCI To Ethernet/Graphics Combo Adapter and will include generic VGA graphics support in the resulting kernel.

### 1.7.2 DEGPA-TA Gigabit Ethernet Device

This patch provides support for DEGPA-TA (1000BaseT) Gigabit Ethernet device. If you have a system with this new Ethernet device, you will need to reconfigure and rebuild the kernel after installing this patch.

To do this, follow these steps:

1. Shut down the system:

   # **/usr/sbin/shutdown -h now**

2. Boot genvmunix to single-user mode:

   >>> **boot -fi genvmunix -fl s**

3. After the system boots to single-user mode, mount the file systems, run the `update` command, and activate the swap partition:

   # **/sbin/bcheckrc**

   # **/sbin/update**

   # **/sbin/swapon -a**

4. Run `doconfig` to create a new kernel configuration file and rebuild the kernel:

   # **/usr/sbin/doconfig**

   **Note**

   Do not specify the `-c` option to `doconfig`. If you do, `doconfig` will use the existing kernel configuration file which will not have the appropriate controller entry for the new graphics card.

5. Save the old `/vmunix` file and move the new kernel to `/vmunix`.

6. Shut down the system:

   # **/usr/sbin/shutdown -h now**

7. Boot the new kernel:

   >>> **boot**

If you remove this patch from your system after you have rebuilt the kernel to incorporate support for the new Ethernet card as described previously, you will need to rebuild the kernel. To do this, follow the steps given previously. The `doconfig` running on the original, unpatched genvmunix will not recognize the new Ethernet driver.

## 1.8 Release Note for Patch 275.00

For more information about the functionality provided and special installation instructions related to Patch 275.00, please refer to the online README file located at:

`http://www.service.digital.com/patches/`

From this URL directory, click on the link that has the name:

`t64v50wlseco2.README`

**Note**

It may be necessary to navigate additional directories below this top-level URL to find the specific `README` file related to this patch.

## 1.9 Release Note for Patches 335.00 and 337.00

This release notes contains the new reference page for `ttauth`.

NAME

ttauth - ToolTalk authority file utility

SYNOPSIS

ttauth [[-f] | [authfile] ] [[-vqib] ] [[command arg ...] ]

DESCRIPTION

The ttauth program is used to edit and display the authorization information used in connecting to ToolTalk. This program is usually used to extract authorization records from one machine and merge them in on another (as is the case when using remote logins or granting access to other users). Commands (described below) may be entered interactively, on the ttauth command line, or in scripts. Note that this program does not contact the ToolTalk server, ttsession. Normally ttauth is not used to create the authority file entry in the first place; ttsession does that.

OPTIONS

The following options may be used with ttauth. They may be given individually or may combined.

-f authfile
This option specifies the name of the authority file to use. By default, ttauth uses the file specified by the TTAUTHORITY environment variable or the .TTauthority file in the user's home directory.

-q This option indicates that ttauth should operate quietly and not print unsolicited status messages. This is the default if an ttauth command is given on the command line or if the standard output is not directed to a terminal.

-v This option indicates that ttauth should operate verbosely and print status messages indicating the results of various operations (for example, how many records have been read in or written out). This is the default if ttauth is reading commands from its standard input and its standard output is directed to a terminal.

-i This option indicates that ttauth should ignore any authority file locks. Normally, ttauth refuses to read or edit any authority files that have been locked by other programs (usually ttsession or another ttauth).

-b This option indicates that ttauth should attempt to break any authority file locks before proceeding. Use this option only to clean up stale locks.

COMMANDS

The following commands may be used to manipulate authority files:

add protoname protodata netid authname authdata
An authorization entry for the indicated ToolTalk session using the given protocol name (protoname), protocol data (protodata), ToolTalk session id (netid), authentication name (authname), and authentication data (authdata) is added to the authorization file. The protocol name should always be the string "TT". The protocol data should always be the empty string. The ToolTalk session ID is formatted string consisting of the ttsession program number, the ttsession authorization level, the IP address of the host running ttsession, and the RPC version number of the ttsession. See the TTSESSION IDENTIFIERS section below for information on constructing ToolTalk session ID's for the authority file. The

authentication name should always be the string "MIT-MAGIC-COOKIE-1". The authentication data is specified as an even-lengthed string of hexadecimal digits, each pair representing one octet. The first digit of each pair gives the most significant 4 bits of the octet, and the second digit of the pair gives the least significant 4 bits. For example, a 32 character hexkey would represent a 128-bit value.

[n]extract filename
Authorization entries which match the specified fields are written to the indicated file. If the nextract command is used, the entries are written in a numeric format suitable for non-binary transmission (such as secure electronic mail). The extracted entries can be read back in using the merge and nmerge commands. If the file name consists of just a single dash, the entries will be written to the standard output.

[n]list
Authorization entries which match the specified fields (or all if nothing is specified) are printed on the standard output. If the nlist command is used, entries are shown in the numeric format used by the nextract command; otherwise, they are shown in a textual format. Key data is always displayed in the hexadecimal format given in the description of the add command.

[n]merge [filename1 ...]
Authorization entries are read from the specified files and are merged into the authorization database, superseding any matching existing entries. If the nmerge command is used, the numeric format given in the description of the extract command is used. If a file name consists of just a single dash, the standard input will be read if it hasn't been read before.

remove
Authorization entries which match the specified fields are removed from the authority file.

source filename
The specified file is treated as a script containing ttauth commands to execute. Blank lines and lines beginning with a pound sign (#) are ignored. A single dash may be used to indicate the standard input, if it has not already been read.

info
Information describing the authorization file, whether or not any changes have been made, and from where ttauth commands are being read is printed on the standard output.

exit
If any modifications have been made, the authority file is written out (if allowed), and the program exits. An end of file is treated as an implicit exit command.

quit
The program exits, ignoring any modifications. This may also be accomplished by pressing the interrupt character.

help [string]
A description of all commands that begin with the given string (or all commands if no string is given) is printed on the standard output.

?
A short list of the valid commands is printed on the standard output.

TTSESSION IDENTIFIERS

The ToolTalk session identifiers (netid) in the authority file and used by the add, [n]extract, [n]list, and remove commands are derived from the TT_SESSION identifier constructed by ttsession at startup. The ttsession rendezvous with clients by writing the TT_SESSION identifier as a property

on the root window or as an environment variable in the client's environment (see ttsession -c). In addition, ttsession creates an entry in the user's authority file. The authority file entry has a netid component which is derived from the TT_SESSION identifier.

The TT_SESSION(STRING) = "01 1433 1342177279 1 1 2002 130.105.9.22 4" identifier is composed of the following elements:

```
 <Dummy Number>                  = 01
 <ttsession Process Id>          = 1433
<ttsession Program Number>       = 1342177279
<DummyNumber>                    = 1
<ttsession Authorization Level>  = 1
<ttsession UID>                  = 2002
<Host IP Address>                = 130.105.9.22
<RPC Version Number>             = 4
```

The ToolTalk session identifiers (netid) in the authority file are composed of the <ttsession Program Number>, <ttsession Authorization Level>, <Host IP Address>, and <RPC Version Number> fields of the TT_SESSION identifier as follows:

1342177279/1/130.105.9.22/4

EXAMPLE

The most common use for ttauth is to extract the entry for the current ttsession, copy it to another machine, and merge it into the user's authority file on the remote machine:

```
% xprop -root | grep TT_SESSION

TT_SESSION(STRING) = "01 1433 1342177279 1 1 2002 130.105.9.22 4"
_SUN_TT_SESSION(STRING) = "01 1433 1342177279 1 1 2002 130.105.9.22 4"

% ttauth extract - netid=1342177279/1/130.105.9.22/4 | rsh otherhost ttauth
merge -
```

ENVIRONMENT

This ttauth program uses the following environment variables:

TTAUTHORITY
Gets the name of the authority file to use if the -f option is not used.

FILES

.TTauthority
Default authority file in the user's home directory if TTAUTHORITY is not defined.

RESTRICTIONS

Users that have unsecure networks should take care to use encrypted file transfer mechanisms to copy authorization entries between machines. Similarly, the MIT-MAGIC-COOKIE-1 protocol is not very useful in unsecure environments. Sites that are interested in additional security may need to use encrypted authorization mechanisms such as Kerberos.

Spaces are currently not allowed in the protocol name. Quoting could be added for the truly perverse.

SEE ALSO

Commands: ttsession(1)

ToolTalk Reference Manual

The options section of the ttsession manpage should now look like this:

-a level
Set the server authentication level. The following level string values are supported:

cookie
The sender and receiver must share the same cookie. This means that messages which do not specify a handler "ptype" are delivered even if the cookies do not match. This is the default authorization scheme. For "full security" use the -F option. Refer to the ttauth(1) reference page for more information.

## 1.10 Release Note for Patch 437.00

This patch contains a solution for the following issue:

Compaq has advised owners of DS10, DS10L, ES40 AlphaServers, and XP900 AlphaStations that Compaq has determined in laboratory testing that there is a theoretical possibility that during read and write operations to the floppy disk on these systems, a single byte of data may be inaccurately read or written without notice to the user or system. The potential for this anomaly exists only if floppy disk read or write operations are attempted while there is extremely heavy traffic on these Alpha systems' internal input/output busses.

Although Compaq has observed the anomaly only in laboratory tests designed to create atypical system stresses, including almost constant use of the floppy disk drive, Compaq has informed owners of the remote possibility that the anomaly could occur so that they may take precautions to prevent it.

Compaq recommends that the solution be installed by all DS10, DS10L, ES40 AlphaServers, and XP900 AlphaStation customers.

The solution to this issue is also available as an individual, manually installed patch kit named `floppy_csp_v50.tar.gz`, available from:

`http://ftp1.support.compaq.com/public/unix/v5.0`

# 2

# Summary of Base Operating System Patches

This chapter summarizes the base operating system patches included in Patch Kit-0003.

Table 2–1 lists patches that have been updated.

Table 2–2 provides a summary of patches in Patch Kit-0003.

**Table 2–1: Updated Base Operating System Patches**

| Patch IDs | Change Summary |
|---|---|
| Patches 151.00, 229.00, 233.00, 235.00, 247.00, 249.00, 251.00, 258.00, 261.00, 265.00, 268.00, 272.00, 288.00, 301.99, 303,00, 311.00, 313.00, 315.00, 319.00, 321.00, 331.00, 333.00, 335.00, 337.00, 339.00, 341.00, 347.00, 349.00, 351.00, 353.00, 355.00, 357.00, 359.00, 361.00, 363.00, 365.00, 367.00, 369.00, 371.00, 373.00, 377.00, 383.00, 385.00, 388.00, 390.00, 396.00, 405.00, 408.00, 410.00, 412.00, 414.00, 416.00, 424.00, 426.00, 428.00, 434.00, 437.00, 439.00, 442.00 | New |
| Patch 131.00 | Superseded by Patch 153.00 |
| Patch 110.00 | Superseded by Patch 155.00 |
| Patches 2.00, 3.00, 6.00, 9.00, 10.00, 13.00, 31.00, 44.00, 47.00, 48.00, 64.00, 80.00, 83.00, 91.00, 93.00, 98.00, 101.00, 108.00, 112.00, 120.00, 127.00, 128.00, 129.00, 65.00, 88.00, 94.00, 97.00, 49.00, 132.00, 114.00, 14.00, 17.00, 74.00, 92.00, 100.00, 103.00, 119.00, 7.00, 139.00, 12.00, 104.00, 96.00, 20.00, 45.00, 51.00, 143.00, 73.00, 5.00, 76.00, 84.00, 113.00, 141.00, 135.00, 4.00, 130.00, 156.00, 157.00, 158.00, 159.00, 160.00, 161.00, 162.00, 163.00, 164.00, 165.00, 166.00, 167.00, 168.00, 169.00, 170.00, 171.00, 172.00, 173.00, 174.00, 175.00, 176.00, 177.00, 178.00, 179.00, 180.00, 181.00, 182.00, 183.00, 184.00, 185.00, 186.00, 187.00, 188.00, 189.00, 190.00, 191.00, 192.00, 193.00, 194.00, 195.00, 196.00, 197.00, 198.00, 199.00, 200.00, 201.00, 202.00, 203.00, 204.00, 205.00, 206.00, 207.00, 208.00, 209.00, 210.00, 211.00, 212.00, 213.00, 214.00, 215.00, 216.00, 217.00, 218.00, 219.00, 220.00, 221.00, 222.00, 223.00 | Superseded by Patch 225.00 |
| Patches 226.00, 227.00 | Superseded by Patch 229.00 |
| Patch 8.00 | Superseded by Patch 231.00 |
| Patches 102.00, 121.00, 236.00, 237.00, 238.00, 239.00, 240.00, 241.00, 242.00, 243.00 | Superseded by Patch 245.00 |
| Patches 136.00, 252.00 | Superseded by Patch 254.00 |
| Patches 255.00, 256.00 | Superseded by Patch 258.00 |
| Patch 259.00 | Superseded by Patch 261.00 |
| Patch 81.00 | Superseded by Patch 263.00 |
| Patch 266.00 | Superseded by Patch 268.00 |
| Patch 32.00 | Superseded by Patch 270.00 |
| Patches 62.00, 273.00 | Superseded by Patch 275.00 |

**Table 2–1: Updated Base Operating System Patches (cont.)**

| | |
|---|---|
| Patches 43.00, 30.00, 95.00, 70.00, 276.00, 277.00, 278.00, 279.00, 280.00 | Superseded by Patch 282.00 |
| Patches 36.00, 58.00, 283.00 | Superseded by Patch 285.00 |
| Patch 286.00 | Superseded by Patch 288.00 |
| Patches 57.00, 34.00, 35.00, 55.00, 289.00, 290.00, 291.00, 292.00, 293.00, 294.00, 295.00, 296.00, 297.00 | Superseded by Patch 299.00 |
| Patches 1.00, 68.00 | Superseded by Patch 305.00 |
| Patches 306.00, 307.00, 308.00, 309.00 | Superseded by Patch 311.00 |
| Patch 77.00 | Superseded by Patch 317.00 |
| Patches 59.00, 63.00 | Superseded by Patch 323.00 |
| Patch 145.00, 147.00 | Superseded by Patch 325.00 |
| Patch 53.00 | Superseded by Patch 327.00 |
| Patches 19.00, 122.00 | Superseded by Patch 329.00 |
| Patches 29.00, 90.00, 342.00 | Superseded by Patch 344.00 |
| Patch 345.00 | Superseded by Patch 347.00 |
| Patches 22.00, 85.00 | Superseded by Patch 375.00 |
| Patch 61.00 | Superseded by Patch 379.00 |
| Patch 146.00 | Superseded by Patch 381.00 |
| Patch 386.00 | Superseded by Patch 388.00 |
| Patches 11.00, 69.00, 79.00 | Superseded by Patch 392.00 |
| Patch 126.00 | Superseded by Patch 394.00 |
| Patches 18.00, 397.00 | Superseded by Patch 399.00 |
| Patch 33.00 | Superseded by Patch 401.00 |
| Patches 402.00, 403.00 | Superseded by Patch 405.00 |
| Patch 406.00 | Superseded by Patch 408.00 |
| Patch 107.00 | Superseded by Patch 418.00 |
| Patches 144.00, 419.00, 420.00 | Superseded by Patch 422.00 |
| Patches 78.00, 148.00 | Superseded by Patch 430.00 |
| Patches 72.00, 106.00, 140.00 | Superseded by Patch 432.00 |
| Patch 435.00 | Superseded by Patch 437.00 |
| Patch 440.00 | Superseded by Patch 442.00 |

**Table 2–2: Summary of Base Operating System Patches**

| Patch IDs | Abstract |
|---|---|
| Patch 16.00<br>OSF500-017 | **Patch:** Fix for stdhosts command<br>**State:** Existing<br>This patch fixes a problem with the stdhosts command when the file processed has lines longer than 256 characters. The following error message is displayed:<br><br>stdhost:malformed line "ignored" |

**Table 2–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 21.00<br>OSF500-024 | **Patch:** Fix for crontab command<br>**State:** Existing<br>This patch fixes a problem with crontab in which, when root runs crontab -e user, the user's crontab file is edited and saved, but is not re-read by the cron daemon. Instead, root's crontab file is re-read. |
| Patch 23.00<br>OSF500-027 | **Patch:** Fix for ksh core dump problem<br>**State:** Supersedes patch OSF500-016 (15.00)<br>This patch corrects the following:<br>• Corrects a problem that may cause ksh to core dump when displaying a large here-document in a ksh script.<br>• Fixes a problem in ksh which required two SIGTERM signals to be sent to the process when it exec'ed. |
| Patch 25.00<br>OSF500-030 | **Patch:** Restriction lifted for AlphaServer DS20 and ES40<br>**State:** Existing<br>This patch removes a Granularity Hint Regions (also called GH chunks) restriction which may be encountered on AlphaServer DS20 and ES40 systems running the Tru64 UNIX 5.0 release. This restriction can reduce performance for certain data base applications. |
| Patch 26.00<br>OSF500-031 | **Patch:** Fix for NFS client application hang<br>**State:** Existing<br>This patch corrects a problem that can cause an NFS client application to hang, or causes a "lock already owned by thread" panic when lockmode=4. |
| Patch 27.00<br>OSF500-035 | **Patch:** Security (SSRT0583Z)<br>**State:** Existing<br>A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability. |
| Patch 28.00<br>OSF500-034 | **Patch:** Fix for binmail<br>**State:** Existing<br>This patch corrects a problem with binmail which was resulting in partial delivery of mail messages when account quota or disk capacity was reached. |
| Patch 37.00<br>OSF500X11-002 | **Patch:** Fix for segmentation fault on X font server (xfs)<br>**State:** Existing<br>This patch fixes a problem where the X font server (xfs) sometimes failed with a segmentation fault when it received an invalid request. |
| Patch 38.00<br>OSF500X11-003 | **Patch:** Fix for problem in X Display Manager (xdm)<br>**State:** Existing<br>This patch fixes a problem in the X Display Manager (xdm) where XDMCP Indirect queries do not work. |
| Patch 39.00<br>OSF500CDE-001A | **Patch:** Fix for dxaccounts shared library<br>**State:** Existing<br>This patch fixes a problem where the Account Manager application, dxaccounts, gets a "BadPixmap" error when selecting an account after the "View Preferences" "Display Icons By Name" option has been selected. |

**Table 2–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 40.00<br>OSF500CDE-002 | **Patch:** Security (SSRT0614U)<br>**State:** Existing<br>A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability. |
| Patch 41.00<br>OSF500CDE-003 | **Patch:** Security (SSRT0571U)<br>**State:** Existing<br>A potential security vulnerability has been discovered where, under certain circumstances, users may gain unauthorized access. Compaq has corrected this potential vulnerability. |
| Patch 42.00<br>OSF500-001 | **Patch:** rc.config and rc.config.common files may be corrupt<br>**State:** Existing<br>This patch fixes a problem where the rc.config and rc.config.common files can be corrupted if the system takes a non-syncing halt after rcmgr updates these files. |
| Patch 46.00<br>OSF500-048 | **Patch:** Fix for simple lock timeout panic<br>**State:** Existing<br>This patch fixes a problem on some AlphaServer GS140/GS60 configurations where a simple lock timeout or TB shoot ack timeout panic may occur. |
| Patch 50.00<br>OSF500CDE-001B | **Patch:** Fix for dxaccounts static library<br>**State:** Existing<br>This patch fixes a problem where the Account Manager application, dxaccounts, gets a "BadPixmap" error when selecting an account after the "View Preferences" "Display Icons By Name" option has been selected. |
| Patch 52.00<br>OSF500CDE-005 | **Patch:** Security (SSRT0615U)<br>**State:** Existing<br>A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability. |
| Patch 54.00<br>OSF500CDE-007 | **Patch:** New windows visible when screen is locked<br>**State:** Existing<br>This patch fixes a problem where when running the Common Desktop Environment (CDE) on a system with more than one graphics card and monitor (multihead). Sometimes new windows were visible when the screen was locked. |
| Patch 56.00<br>OSF500DX-005 | **Patch:** Fix for Insight Manager configuration tool<br>**State:** Existing<br>The Insight Manager configuration tool now correctly operates on the remote cluster node being configured. Previously, changes would not take affect until Insight Manager was restarted manually on the remote node. |
| Patch 66.00<br>OSF500-102 | **Patch:** Fix for unaligned access panic in dli_input<br>**State:** Existing<br>This patch fixes an unaligned access panic in dli_input. |

**Table 2–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 71.00<br>OSF500-107 | **Patch:** Corrects a problem with the compress utility<br>**State:** Existing<br>This patch corrects a problem with the (un)compress utility which could result in either an incomplete compressed file and loss of the original uncompressed file, or an incomplete uncompressed file and loss of the original compressed file. |
| Patch 75.00<br>OSF500-111 | **Patch:** NIS client has a different shell listed than server<br>**State:** Existing<br>This patch corrects a problem where an NIS client has a different shell listed for an NIS user than does the server. When the user tried to change their NIS password, the password change failed, but the shell was updated. |
| Patch 82.00<br>OSF500-119 | **Patch:** Fixes callback on freed CCB panics<br>**State:** Existing<br>This patch fixes callback on freed CCB panics. |
| Patch 86.00<br>OSF500-123 | **Patch:** Security (SSRT0592U)<br>**State:** Existing<br>A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability. |
| Patch 87.00<br>OSF500-124 | **Patch:** In C2 environment imap authentication fails<br>**State:** Existing<br>This patch corrects a problem where, in an enhanced security (C2) environment, imap authentication fails. |
| Patch 89.00<br>OSF500-126 | **Patch:** sendmail core dumps sending 8-bit mime-encoded files<br>**State:** Existing<br>Fixes a problem where sendmail core dumped when trying to send certain 8-bit, mime-encoded files. |
| Patch 99.00<br>OSF500-032 | **Patch:** Fix for AS1200 systems with multiple memory cards<br>**State:** Existing<br>This patch fixes a problem where AS1200 systems with more than three pairs of memory cards display the following warning on the console during boot:<br><br>pmap_get_align: Unaligned memory hole found...<br>Please reset the system to clear any previous memlimit |
| Patch 109.00<br>OSF500-060 | **Patch:** Fix for lex problems<br>**State:** Existing<br>This patch fixes a problem in lex that causes it to generate incorrect tables that result in the lexical analyzer failing to recognize some kinds of regular expressions involving exclusive start states. |
| Patch 111.00<br>OSF500-062 | **Patch:** Fix for news command<br>**State:** Existing<br>This patch fixes a problem in which the news command fails due to the appending of additional characters to file names in the /usr/news directory. |
| Patch 115.00<br>OSF500-066 | **Patch:** Fix for rpc.statd hang<br>**State:** Existing<br>This patch fixes a problem where rpc.statd hangs as it tries to notify dead remote systems. |

**Table 2–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 116.00<br>OSF500-067 | **Patch:** mailsetup does not complete if hostname ends in zero<br>**State:** Existing<br>This patch fixes a problem of not completing mailsetup if the hostname ends with 0 (zero). The error message produced follows:<br>Error creating /var/adm/sendmail/.cf: exiting |
| Patch 117.00<br>OSF500-071 | **Patch:** lprsetup incorrectly sets up certain printers<br>**State:** Existing<br>This patch fixes a problem where the lprsetup command would incorrectly set up certain types of printers, such as the hp1120c, hp4000tn, or hp61. |
| Patch 123.00<br>OSF500-078 | **Patch:** Fixes core dump problem with ftp<br>**State:** Existing<br>This patch fixes a core dump problem with ftp(1) when a .netrc file contains an invalid macdef (macro definition). |
| Patch 124.00<br>OSF500-079 | **Patch:** Fixes problem with fverify -n flag<br>**State:** Existing<br>This patch fixes a problem with the fverify -n flag creating directories. |
| Patch 133.00<br>OSF500-088 | **Patch:** Fixes a problem with the KZPSA driver<br>**State:** Supersedes patches OSF500-072 (118.00), OSF500-080 (125.00)<br>This patch corrects the following:<br>• Fixes a problem with the KZPSA driver. A timer is not being canceled causing a panic with the following error message:<br>xpt_callback: callback on freed CC<br>• Fixes a problem in which the system can panic with the following message:<br>KZPSA PANIC SPO_RET_CARRIER:CARRIER NOT IN USE<br>• Fixes a problem with tmv2_notify_cbf messages being logged from KPBSA adapters and creating very large binary.errlog files in a clustered environment. |
| Patch 134.00<br>OSF500-089 | **Patch:** Fix for joind problem<br>**State:** Supersedes patches OSF500-103 (67.00), OSF500-055 (105.00)<br>This patch corrects the following:<br>• Fixes a problem in which joind does not listen on interfaces configured with DECnet and returns "unaligned access" messages.<br>• Fixes a problem with the joind daemon not appending the hostname to the load file specified in the bf flag in the /etc/bootptab file.<br>• Fixes a problem in which bprelay does not work properly and displays the error message "bprelay[658]: can't find interface which received packet". |
| Patch 137.00<br>OSF500-092 | **Patch:** Corrects a disk write failure<br>**State:** Existing<br>This patch corrects a Disk write failure when using the -swap option and the simple disk on the original disk starts at offset 0. |

**Table 2–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 138.00<br>OSF500-093 | **Patch:** Fix for ris script<br>**State:** Existing<br>This patch corrects the following problems with the /usr/sbin/ris script:<br>• It incorrectly queried the user for a gateway to be used to serve a specific client when no gateway was required.<br>• It could fail if no default route had been established. |
| Patch 142.00<br>OSF500-097 | **Patch:** Fixes system hang due to problem in NFS write code<br>**State:** Supersedes patch OSF500-029 (24.00)<br>This patch corrects the following:<br>• Corrects problems with NFS V3 XDR encoding. It also corrects a problem where the system may hang due to a problem with NFS write gathering code.<br>• Fixes a system hang problem due to a bug in the nfs write gathering code. The code does not fully synch all writes. |
| Patch 149.00<br>OSF500-065B | **Patch:** Corrects problems in AdvFS propertly list handling<br>**State:** Existing<br>This patch corrects two problems in AdvFS property list handling:<br>• Creation of property lists entries in AdvFS filesets with no available mcells will result in kernel memory fault (kmf).<br>• The get_proplist_entry function (used to disassemble the property list buffer returned by the getproplist system call) returned an incorrect name length on property list names longer than 127 characters. |
| Patch 151.00<br>OSF500-253 | **Patch:** Corrects problem in the LAT driver<br>**State:** New<br>This patch corrects a problem in the LAT driver which caused improper processing of the ioctl TCSBRK as well as the generation of spurious <BREAK> characters when the libc routine tcdrain() was used. |

**Table 2–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 153.00<br>OSF500-220 | **Patch:** Fix for vrestore command<br>**State:** Supersedes patches OSF500-086 (131.00)<br>This patch fixes the following problems in the vrestore command:<br>• vrestore is slow to complete when a partial restore operation is requested.<br>• vrestore fails to ignore extended attribute records for those files that are not requested in a vrestore operation.<br>• vrestore fails to restore certain files and directories having ACLs from a compressed vdump saveset, reporting:<br>vrestore: error setting extended attributes 22<br>• A previous patch caused incomplete restores.<br>• A warning message is displayed when the path for the first file in a group of hardlinks is created without using original protection codes and property lists.<br>• A warning message is displayed and vrestore aborts if it fails to malloc space for a property list.<br>• A message which had been inserted at the end of the message file had the wrong message category (this could cause messaging confusion).<br>• An uninitialized variable in the code that restores property lists could cause malloc failures, memory faults, "error setting extended attributes," and infinite loops using the -l option.<br>• Corrupted property list information could cause an infinite loop. |
| Patch 155.00<br>OSF500-224 | **Patch:** Fixes problem in kernel debugger, kdbx<br>**State:** Supersedes patches OSF500-061 (110.00)<br>This patch fixes a problem in the kernel debugger, kdbx, where several commands, particularly list_action and slot, are broken. Other commands such as mount-action and array_action that rely on list_action will also fail. This patch fixes problems with the kdbx extensions mount and swap. Information about the file system type is incorrect in the mount command. The device name is missing in the swap command. |

**Table 2–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 225.00<br>OSF500-166 | **Patch:** Security (SSRT0675U)<br>**State:** Supersedes patches OSF500-003 (2.00), OSF500-004 (3.00), OSF500-007 (6.00), OSF500-010 (9.00), OSF500-011 (10.00), OSF500-014 (13.00), OSF500-038 (31.00), OSF500-040 (44.00), OSF500-049 (47.00), OSF500-053 (48.00), OSF500-100 (64.00), OSF500-117 (80.00), OSF500-120 (83.00), OSF500-128 (91.00), OSF500-130 (93.00), OSF500-143 (98.00), OSF500-045 (101.00), OSF500-059 (108.00), OSF500-063 (112.00), OSF500-074 (120.00), OSF500-082 (127.00), OSF500-083 (128.00), OSF500-084 (129.00), OSF500-101 (65.00), OSF500-125 (88.00), OSF500-131 (94.00), OSF500-139 (97.00), OSF500-054 (49.00), OSF500-087 (132.00), OSF500-065A (114.00), OSF500-015 (14.00), OSF500-018 (17.00), OSF500-110 (74.00), OSF500-129 (92.00), OSF500-039 (100.00), OSF500-051 (103.00), OSF500-073 (119.00), OSF500-008 (7.00), OSF500-094 (139.00), OSF500-013 (12.00), OSF500-052 (104.00), OSF500-138 (96.00), OSF500-022 (20.00), OSF500-046 (45.00), OSF500-069 (51.00), OSF500-098 (143.00), OSF500-109 (73.00), OSF500-006 (5.00), OSF500-113 (76.00), OSF500-121 (84.00), OSF500-064 (113.00), OSF500-096 (141.00), OSF500-090 (135.00), OSF500-005 (4.00), OSF500-085 (130.00), OSF500-219 (156.00), OSF500-180 (157.00), OSF500-263 (158.00), OSF500-232 (159.00), OSF500-236 (160.00), OSF500-155 (161.00), OSF500-274 (162.00), OSF500-251 (163.00), OSF500-151 (164.00), OSF500-153 (165.00), OSF500-255 (166.00), OSF500-285 (167.00), OSF500-257 (168.00), OSF500-276 (169.00), OSF500-241 (170.00), OSF500-145 (171.00), OSF500-167 (172.00), OSF500-149 (173.00), OSF500-181 (174.00), OSF500-281 (175.00), OSF500-235 (176.00), OSF500-289 (177.00), OSF500-238 (178.00), OSF500-150 (179.00), OSF500-243 (180.00), OSF500-133 (181.00), OSF500-175 (182.00), OSF500-231 (183.00), OSF500-194 (184.00), OSF500-140 (185.00), OSF500-279 (186.00), OSF500-261 (187.00), OSF500-163 (188.00), OSF500-298 (189.00), OSF500-270 (190.00), OSF500-262 (191.00), OSF500-152 (192.00), OSF500-284 (193.00), OSF500-209 (194.00), OSF500-227 (195.00), OSF500-165 (196.00), OSF500-265 (197.00), OSF500-269 (198.00), OSF500-234 (199.00), OSF500-272 (200.00), OSF500-216 (201.00), OSF500-169 (202.00), OSF500-132 (203.00), OSF500-210 (204.00), OSF500-193 (205.00), OSF500-278 (206.00), OSF500-197 (207.00), OSF500-162 (208.00), OSF500-157 (209.00), OSF500-211 (210.00), OSF500-222 (211.00), OSF500-159 (212.00), OSF500-268 (213.00), OSF500-137 (214.00), OSF500-237 (215.00), OSF500-206 (216.00), OSF500-161 (217.00), OSF500-250 (218.00), OSF500-173 (219.00), OSF500-142 (220.00), OSF500-198 (221.00), OSF500-296 (222.00), OSF500-271 (223.00<br>This patch corrects the following:<br>• Fixes "simple_lock: time limit exceeded" panics.<br>• Fixes a panic in the kernel with the following error message:<br>simple_lock: time limit exceeded<br>• Fixes a problem that causes the Tru64 UNIX Version 5.0 update install procedure to exit with core dumps and /sbin/loader failures on a system.<br>• Fixes a problem where applications using the fcntl() system calls may appear to hang.<br>• Fixes a "lock hierarchy violation" panic from running "fuser -d" command on AdvFS when lockmode is set to 4.<br>• Fixes a problem where process accounting data was not written to the accounting file when the accounting file was on an NFS-mounted file system. |

**Table 2–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 225.00 continued | • Fixes a system "pause" seen when doing a lot of I/O to UFS filesystems.<br>• Fixes system hangs that occur when there are nfs mounted files, the system is actively paging and the nfs server is unavailable.<br>• Fixes a "page owner not valid" system panic or a system hang on large memory systems. This can be seen when SSM objects are created and accessed on systems experiencing heavy paging and swapping activity.<br>• Fixes an AdvFS problem in which processes may hang but the system will not panic.<br>• Fixes problems in the AdvFS file system. The problems included an EBUSY unmount problem and a panic that occurred when executing bs_real_invalidate_pages().<br>• Fixes a problem in which unmounting an NFS mounted directory can cause a user process to core dump.<br>• Fixes a problem with hangs on AlphaServer ES40 when specifying granularity hints.<br>• Fixes a problem where ubc_msync() may not flush out all the pages in the requested range.<br>• Fixes a problem involving register corruption.<br>• Fixes var adm messages from truncation on larger configurations by raising the default size (4096) of msgbuf_size to 8192.<br>• Fixes a problem where systems with Patch Kit-0001 installed would run low on kernel memory after process accounting had been running for a while.<br>• Fixes a problem with soclose() that caused permanent looping on exit while aborting pending connections at a TCP/IP listener socket.<br>• Fixes a problem that could result in a incorrect scheduling of threads when they were dispatched from the idle state. |

**Table 2–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 225.00 continued | • Fixes a problem with virtual memory. When running the Oracle database, Oracle can not detach from a shared memory segment.<br>• Fixes two separate panics with the following error messages:<br>vm_page_activate: already active<br>or<br>simple_lock: time limit exceeded<br>• Fixes a simple_lock: hierarchy violation in sigq_abort() when lockmode is set to 4.<br>• Adds the following kernel features:<br>– Enhanced core path support which allows applications to specify the directory where core files will be generated.<br>– XA_FORK exit action support which allows applications to register actions to be performed when a process forks().<br>• Corrects a problem in which a "device busy" error would be reported; the behavior has been changed to wait for the busy pages to be released.<br>• Fixes a problem in the AdvFS system. A panic occurs with the following error message:<br>lock_read: hierarchy violation<br>• Fixes a problem where a single CPU system using AdvFS can hang in cleanup_closed_list().<br>• Fixes a problem where several 8K pages in a file on an AdvFS filesystem can incorrectly contain all zeros instead of the data that was written to that portion of the file.<br>• Corrects an AdvFS problem involving clone filesets. The read-ahead code was incorrectly passing up opportunities to do read-ahead on clone filesets, resulting in a large performance penalty.<br>• Fixes a problem with making a msfs_putpage() call. The length argument may get its upper bits truncated which will result in an incorrect length calculation.<br>• Corrects two problems in AdvFS property list handling:<br>– Creation of property lists entries in AdvFS filesets with no available mcells will result in kernel memory fault (kmf).<br>– The get_proplist_entry function (used to disassemble the property list buffer returned by the getproplist system call) returned incorrect name length on property list names longer than 127 characters.<br>• Corrects a hang of the FDDI interface if the interface is brought down following a read-and-zero-counters request (netstat -z on the FDDI interface, for example).<br>• Fixes a kernel memory fault and an SMP race condition with the AltaVista Firewall 98 server on a multi-CPU system.<br>• Fixes a problem in which the system may panic with the error message "kernel memory fault".<br>• Fixes a system panic:<br>tcphdr too big |

**Table 2–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 225.00 continued | • Changes necessary for AV firewall 98 to pass ICSA certification.<br>• Fixes a kernel memory fault caused when a network application walked an inpq array.<br>• Fixes a problem where RCP commands issued from a Sun Solaris system to Compaq Tru64 UNIX may sometimes fail incorrectly with the error message:<br>Connection reset by peer<br>• Fixes a problem in which the system may panic with the error message:<br>tcp_output REXMT<br>• Fixes a TCP performance problem if the TCP window scale option is turned off when using the HIPPI interface.<br>• Fixes a problem with packetfilter applications that use ip packets greater than 8K.<br>• Corrects a problem where ICMP redirect packets can modify the default route.<br>• This patch involves virtual mac addressing.<br>• Fixes a kmf problem when the type of SCSI device dynamically changes.<br>• Fixes an error in the SCSI device probe code. On systems with shared bus configurations, heavy I/O loads can cause duplicate device files to be created for the same device.<br>• Fixes a hardware management problem that will cause a system hang at boot time (in dsfmgr) whenever a hardware CPU upgrade is performed.<br>• Fixes a problem in which the system can panic with a kernel memory fault.<br>• Fixes a problem where partitioned AlphaServer 8200/8400 systems return incorrect CPU data for CPUs that are not in the partition.<br>• Fixes the following Compaq AlphaServer problems:<br>– On the ES40 and DS20, nonfatal 680 environment machine checks are being logged as fatal/noncorrectable errors.<br>– On the DS20, a fix has been made to the handling of power supply, temperature, and fan events so that they are reported correctly.<br>– Provides support for the Compaq AlphaServer DS20E. |

**Table 2–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 225.00 continued | • Allows the com1_environment variables to be stored in NVRAM. On a DS10 platform, when resetting console baud rate to anything other than the rate it was running, a system panic occurs at boot.<br>• Corrects siginfo codes for floating point and integer overflow exceptions.<br>• Fixes single-step support in a debugger, such as Ladebug, for instructions that trap or fault.<br>• Fixes a problem where registers might be corrupted with the preemption_on/off interfaces.<br>• Fixes a problem which could result in unit attention status being missed.<br>• Fixes the following Universal Serial Bus (USB) problems:<br>– The USB mouse no longer functions after resetting the Xserver.<br>– System panics may occur in error handling after USB device fails a request.<br>– The USB device may not deconfigure properly when unplugged from the bus.<br>– Problems that will prevent some USB devices from being configured at boot time.<br>– A key on a USB keyboard will continue to repeat after being unplugged.<br>– USB keyboards may transmit the incorrect keycode for several keys.<br>• When booting at times the USB controller number may be -1. This causes doconfig to fail. |

**Table 2–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 225.00 continued | • Includes UFS "delayed" metadata mount option that fixes metadata intensive application performance.<br>• Fixes a panic in the UFS filesystem which has the following error message:<br>blkfree: freeing free block<br>• Fixes a problem in which operations on NFS files can hang indefinitely.<br>• Fixes a problem in which a reboot will fail after hwmgr is used to delete or add devices.<br>• Fixes a problem in which a reboot will fail after hwmgr is used to delete or add devices.<br>• Fixes a system hang that can occur during an NFS operation on a system running granularity hints.<br>• Addresses a binary comptibility problem seen with four networking system calls: sendmsg, osendmsg, recvmsg, and orecvmsg. In certain cases, executables compiled on other versions of TRU64 UNIX will not work correctly when using these system calls.<br>• Corrects a problem with four networking system calls, sendmsg/osendmsg and recvmsg/orecvmsg. Anyone of these calls may return an unexpectedly large negative value.<br>• Fixes the following two filesystem problems:<br>– In AdvFS, a system panic with the following error message:<br>panic: bs_logflush_start: cannot write lsn<br>– NFS errors are recieved when doing file I/O on an AdvFS exported file system.<br>• Fixes a panic in in_pcbfree() when NFS is implemented over TCP.<br>• There is a potential for a system panic in routine sbflush() if there is an attempt to flush a socket buffer while it is locked by another thread. This patch corrects this problem.<br>• Fixes a problem with AdvFS where all processes are waiting for buffers causing the system to hang.<br>• Fixes two panics that have the following error messages:<br>simple_lock: time limit exceeded<br>simple_lock: lock already owned by cpu<br>• Fixes a problem in which, when opening a RAID type device, the ALL_DTYPE_RAID was not being allowed.<br>• Fixes a problem in which the system can hang if there is no CPU in slot 0. It also fixes an instruction fault due to a divide by 0. |

**Table 2–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 225.00 continued | • Fixes a problem where, if the size of the message queue was increased, writers to the queue that were blocked would not wake up for processing.<br>• Fixes a problem that causes corruption in the floating point registers whereby the flag fields nxm_fp_owned are overwritten with 0s.<br>• Fixes a problem with verify. When verify is run on a brand new domain, NFS warnings are displayed even though no NFSrelated activity is being done.<br>• Fixes a problem in AdvFS. When calling bs_startio, the wrong number of parameters was being used, resulting in a potential slow down of some flushes.<br>• Fixes the following two problems in the I/O subsystem:<br>– Only the first byte of the HSZ serial number is checked.<br>– tThe time allowed for the command timeout on AIT tape drives is increased to from 5 seconds to 5 minutes.<br>• Fixes a problem in AdvFS. The function bfflush_range() may return success before flushing all the pages it should.<br>• Fixes a race condition in the UBC code where a lookup is done on a page being invalidated (freed).<br>• fixes a kernel memory fault in VMAC code if_addnewaddr().<br>• Corrects a problem which could cause the system to spend excessive time in the internet checksum routine, resulting in a degradation of system performance.<br>• Fixes a problem with VM page corruption that has the following panic message:<br>vm_pg_alloc: page not free<br>• Fixes a panic which has the following error message:<br>simple_lock: hierarchy violation<br>• Fixes "can_replace: slot replacement mismatch" panics which can occur when running multithreaded applications.<br>• Fixes a panic which has the following error message:<br>lock_clear_recursive: recursion not enabled<br>• Fixes a problem in which metadata buffers are being written asynchronously instead of on a delayed basis.<br>• Fixes a problem in AdvFS where v_numoutput is not being decremented, causing AdvFS to hang.<br>• Corrects a problem when a network interface is configured using a CIDR bitmask and lies in a certain address range; it could be unreachable by users on the local system and remote systems that choose not to use the routing table but simply transmit on an interface.<br>• Fixes a problem in which network deamons, such as NIS and NFS, do not function properly because of mislabeled packets.<br>• Fixes a hang or simple_lock_state_violation/simple_lock_fault panic in biodone.<br>• Fixes a problem that caused an incorrect bcache size to be returned to the kernel from the HWRPB. This problem occurred on Professional Workstation 900 and 1000 systems and AlphaServer DS10, DS20, DS20E, ES40, GS80, GS160, and GS320 systems. |

**Table 2–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 225.00 continued | • Prevents a deadlock in NFS over TCP that could occur if the client is not responding properly. The hang will be seen in the nfs tcp threads in rrok3free().<br>• This patch fixes a system panic with panic string:<br>psig: catch not set<br>• Fixes a problem where some network based multimedia applications will cause a kernel memory fault when exiting.<br>• Fixes a "lock_terminate: lock held" panic when deleting a process group.<br>• Fixes a kernel memory fault caused by either one of the following conditions:<br>– On EV6 platforms, when the debugger is used to view the OT_DEVMAP object mapping memory in I/O space that is mapped to a user process.<br>– When routine pmap_coproc_exit_notify() modifies the pmap's coproc_tbi function to be 0, a null pointer, while it is being checked by routine pmap_remove_all().<br>• Fixes a problem in AdvFS. A panic occurs with the following error message:<br>lock_read: hierarchy violation<br>• Fixes a problem with AdvFS. An AdvFS domain becomes inaccessible when using the mount -d option.<br>• Fixes a problem in AdvFS in which a system that had already domain paniced results in a system panic.<br>• Provides support for an increase in the number of binlog records for FRU/config tables to greater than 32K.<br>• Corrects several cam device related problems.<br>– The ddr database entry for HSG80 is now handled correctly by the .mrg file.<br>– A kernel memory fault while performing HSZ80 failover has been corrected<br>– The RA3000 (HSZ22) now correctly reports the value for AWRE/ARRE in the error page.<br>– Corrects a problem that caused HSG70 or HSG80 pairs to fail to respond to selection when performing a transparent failover from one controller to another. Prior to this patch, the HSG70 or HSG80 pairs were unable to see paths to devices; consequently the devices were declared unreachable.<br>• Fixes a race condition involving signals and threads that only happens on multiprocessor systems.<br>• Fixes a problem in which the POSIX interval timer is not resilent to clock slowdown cause either by NTP or by a backwards change of the clock.<br>• Fixes a bug such that, when fuser - is issued on a dismounted NFS mount point in which some process is running, a hang will occur.<br>• Fixes an "unaligned kernel space access from kernel mode" panic when doing a malloc from kmembucket 26, 896 byte bucket. The faulting virtual address will be the lock signature for thread_deallocate(). |

**Table 2–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 225.00 continued | • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability.<br>• Fixes a problem in AdvFS where user data may be lost when a clone file is migrated.<br>• Fixes a problem where a root user was not allowed to check file access on behalf of a user without completely becoming the user. The functionality is needed by the ASU (Advanced Server for UNIX) product.<br>• Fixes a problem in which an application can hang because of an undelivered signal.<br>• Fixes a problem in which an application can hang because of an undelivered signal.<br>• Fixes a problem in which an application can hang because of an undelivered signal.<br>• Fixes a problem where the operating system only looks in slot 0 for the primary CPU.<br>• Fixes a problem where the hardware manager reports inaccurately the CPU speed.<br>• Fixes a problem with AdvFS in which a hang occurs due to a deadlock between bsbuf.state and bmt extent map lock.<br>• Fixes a problem in which an invalid error status is returned from the remove_entry system call.<br>• Corrects a kermel memory fault caused by hwmgr.<br>• Fixes a kernel memory fault seen under certain conditions when setting a thread's priority.<br>• Fixes a problem where, in the output of a ps command, the PAGEIN column reports 0 for all processes.<br>• Fixes support of converting bootable tape bootstrings to device names and converting device names back to bootable tape bootstrings.<br>• Fixes several panics on systems with holes in memory. The error messages are listed below:<br>panic: put_free_ptepage: invalid pvh state<br>panic: kernel memory fault<br>trap: invalid memory read access from kernel mode<br>panic: not wired<br>simple_lock: hierarchy violation<br>• Fixes a problem in which the SCSI version number was not checked for SCSI-3 device. With this patch, SCSI-2 and SCSI-3 devices are checked.<br>• Fixes a panic in in_pcbfree() associated with ASE service failover.<br>• Fixes panics and memory corruption in setuid/setgid.<br>• Corrects a problem where, under certain unlikely conditions, a b-tree index for a directory could become corrupted.<br>• Fixes a problem where the system appears to hang. A child process is holding a lock too long and preventing other processes for doing work. |

**Table 2–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 229.00<br>OSF500-208A | **Patch:** Fix for dbx<br>**State:** New. Supersedes patches OSF500-214 (226.00), OSF500-221A (227.00)<br>This patch fixes the following problems in dbx:<br>• Fixes two problems in dbx:<br>– Dbx stack trace is incomplete.<br>– Assignment to a variable would fail after viewing a non-local symbol.<br>• Fixes a segmentation fault problem with the profiling tool prof. The problem is in library routines that access the line number information in the symbol table, and can affect other commands that look at the symbol table.<br>• Fixes a problem with two routines in the libst library, st_obj_open() and st_obj_write(). The ability to change a file permission using these two libst routines is denied if group has write permissions. |
| Patch 231.00<br>OSF500-221B | **Patch:** prof -pixie -asm command core dumps<br>**State:** Supersedes patches OSF500-009 (8.00)<br>This patch corrects the following:<br>• Fixes a problem where prof -pixie -asm would dump core if the executable being profiled contains extremely long symbol names.<br>• Fixes a segmentation fault problem with the profiling tool prof. The problem is in library routines that access the line number information in the symbol table, and can affect other commands that look at the symbol table. |
| Patch 233.00<br>OSF500-208B | **Patch:** Fix for libst library<br>**State:** New<br>This patch fixes a problem with two routines in the libst library, st_obj_open() and st_obj_write(). The ability to change a file permission using these two libst routines is denied if group has write permissions. |
| Patch 235.00<br>OSF500X11-022 | **Patch:** Support for Euro character to keymap files<br>**State:** New<br>This patch adds support for the Euro character to keymap files. |

**Table 2–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 245.00<br>OSF500-242 | **Patch:** Security (SSRT0636U)<br>**State:** Supersedes patches OSF500-047 (102.00), OSF500-075 (121.00), OSF500-294 (236.00), OSF500-245 (237.00), OSF500-204 (238.00), OSF500-191 (239.00), OSF500-280 (240.00), OSF500-233 (241.00), OSF500-156A (242.00), OSF500-288 (243.00)<br>This patch corrects the following:<br>• Fixes a problem in which ufs_fsck can get blocked while attempting to flush NFS buffers for a service that has become suspended.<br>• Fixes a problem that was causing the csh globbing function to be extremely slow when accessing file information on NFS, AFS, or VMS file systems.<br>• Fixes a problem for those applications that assume initial allocations of memory from the C run-time library's malloc() function will return only zero-filled memory.<br>• Fixes a problem in libc that affects debugger tracebacks of code containing "split procedures".<br>• Fixes a problem in libc where gmtime() would return a tm struct containing an incorrect tm_zone abbreviation if previous calls to both gmtime() and localtime() were made.<br>• Fixes regressions in the regular expression logic used by grep.<br>• Fixes a problem in libc that affects the mktemp, tmpnam, and tempnam functions. The temporary file names that were generated might contain the # charater, which violates the file-naming standard and may cause problems if a shell script containing a reference to that filename is generated.<br>• Corrects the problem with /usr/bin/login in an NIS environment to better handle group information processing.<br>• A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability.<br>• This patch fixes a problem where a TZ environment variable setting of ":" yields incorrect (or missing) time zone information after calling tzset() and incorrect error reporting from mktime().<br>• Adds functionality to terminate the resulting string from calls to swprintf(). |
| Patch 247.00<br>OSF500-156B | **Patch:** Security (SSRT0636U)<br>**State:** New<br>A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability. |
| Patch 249.00<br>OSF500-258 | **Patch:** Fix for umount command<br>**State:** New<br>This patch prevents "not currently mounted" warning messages from being displayed for file systems you did not request to umount. |
| Patch 251.00<br>OSF500-228 | **Patch:** Fix for DECevent Version 3.2<br>**State:** New<br>This patch fixes a problem with DECevent Version 3.2, where the evmshow -d command and the SysMan event viewer will hang when attempting to translate binary error log events. |

**Table 2–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 254.00<br>OSF500-239 | **Patch:** sysconfigtab can cause system to be unbootable<br>**State:** Supersedes patches OSF500-091 (136.00), OSF500-184 (252.00)<br>This patch corrects the following:<br>• Fixes a problem in which an invalid PCI entry in sysconfigtab can cause the system to be unbootable.<br>• Fixes several problems specific to AlphaServer 1200 and AlphaServer 4100 systems:<br>– The user.log file has the following message:<br>redundant power supply failure<br>– The messages file has the following intermittent messages:<br>ERROR: i2c_read_temp: environmental monitoring error<br>ERROR: i2c_read_fail_reg: environmental monitoring error<br>ERROR: i2c_read_func_reg: environmental monitoring error<br>– Systems were shutting themselves down displaying the following message:<br>System has reached a high temperature condition.<br>Possible problem source: Clogged air filter or high ambient room temperature<br>• Provides PCI Resource Management support for the Atalla AXL200 cryptographic accelerator card. It also fixes a problem where genvmunix does not boot on a system with a Atalla AXL200 card installed. |
| Patch 258.00<br>OSF500-199 | **Patch:** Fix for grep command<br>**State:** New. Supersedes patches OSF500-182 (255.00), OSF500-196 (256.00)<br>This patch corrects the following:<br>• Fixes a problem with the grep command in which the options -p -v together does not produce any output.<br>• Corrects a problem with the fgrep command; when it is used with the -s flag all output is suppressed.<br>• Fixes a limitation problem with the grep and fgrep commands. If the line length is too long, grep displays a "wordlist too large" error message, and fgrep displays "input too long" error message. |
| Patch 261.00<br>OSF500-217 | **Patch:** Fix for btcreate command<br>**State:** New. Supersedes patches OSF500-172 (259.00)<br>This patch corrects the following:<br>• Fixes a problem with the btcreate command where default restore fails if disklabel is different.<br>• Fixes a problem with btcreate not waiting long enough for the next tape to be loaded with some media changers. |
| Patch 263.00<br>OSF500-290 | **Patch:** showfdmn sometimes core dumps<br>**State:** Supersedes patches OSF500-118 (81.00)<br>This patch corrects the following:<br>• Fixes a problem in which advfs showfdmn would sometimes core dump.<br>• Fixes two separate problems with vdf:<br>– vdf does not run at non-root level.<br>– vdf may give incorrect information. |

**Table 2–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 265.00<br>OSF500-200 | **Patch:** Fix for find command<br>**State:** New<br>This patch fixes a problem with the find command. Find fails to show filenames that start with a period. |
| Patch 268.00<br>OSF500-176 | **Patch:** Fix for ATM atm_cmm_connect API routine<br>**State:** New. Supersedes patches OSF500-148 (266.00)<br>This patch corrects the following:<br>• Fixes a problem in the ATM atm_cmm_connect API routine when trying to create a VC.<br>• Fixes a kernel memory fault when using ATM. |
| Patch 270.00<br>OSF500-205 | **Patch:** Fix for tar/pax program<br>**State:** Supersedes patches OSF500-043 (32.00)<br>This patch corrects the following:<br>• The tar/pax program did not always read the last tape record of an archive. This caused confusion for scripts that were reading a series of archives on the no-rewind device.<br>• Fixes a cpio hanging problem in the Japanese locales. |
| Patch 272.00<br>OSF500-229 | **Patch:** Fix for incorrect cursor display<br>**State:** New<br>This patch fixes a problem where the cursor is displayed incorrectly when the image plane is set to 1 and the mask plane is set to 0. |
| Patch 275.00<br>OSF500X11-014 | **Patch:** Implements Xlocales definitions<br>**State:** Supersedes patches OSF500X11-008 (62.00), OSF500X11-013 (273.00)<br>This patch corrects the following:<br>• Implements Xlocales definitions that allow X applications to run under the ISO8859-15 locales. Using ISO8859-15 locales allows users to enter and use newly defined ISO8859-based characters such as the Euro monetary symbol.<br>• Provides missing compose definitions when in ISO8859-15 based locales for the scaron, Scaron, zcaron, and Zcaron characters.<br>• Fixes a problem where all the LATIN-9 characters except ASCII characters are not drawn in LATIN-9 (ISO8859-15) locale. |

**Table 2–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 282.00<br>OSF500-240 | **Patch:** Upgrade to Gigabit Ethernet driver Version 1.0.12<br>**State:** Supersedes patches OSF500-033 (43.00), OSF500-037 (30.00), OSF500-135 (95.00), OSF500-106 (70.00), OSF500-170 (276.00), OSF500-293 (277.00), OSF500-186 (278.00), OSF500-295 (279.00), OSF500-299 (280.00)<br>This patch corrects the following:<br>• Corrects a problem where a Tru64 UNIX NFS server incorrectly handles > 8k I/O requests.<br>• Fixes a system panic with the panic string:<br>simple_lock: time limit exceeded<br>• Provides the graphics driver support for the PCI To Ethernet/Graphics Combo Adapter (3X-DEPVD-AA) (also known as the ITI6021E Fast Ethernet NIC 3D Video Combination Adapter, InterServer Combo, or JIB).<br>• Upgrades to the Gigabit ethernet driver Version 1.0.12 to fix various performance problems.<br>• Provides the latest driver for the PowerStorm 4D10T (ELSA Gloria Synergy, SN-PBXGK-BB) graphics card and the latest graphics driver for the PCI To Ethernet/Graphics Combo Adapter (3X-DEPVD-AA).<br>• Prevents a possible NFS over TCP hang. NFS TCP threads will be blocked in sosbwait() causing the system to appear to be hung.<br>• Updates the DE602 ethernet driver to V1.0.5 and fixes the following three driver problems and adds support for the DE602-FA device:<br>– Transmit Timeout errors following adapter reset or loss of link connection.<br>– Kernel memory fault panic on system experiencing many Receive Overrun errors.<br>– Multicast addresses not being received by device.<br>• Provides support for the DEGPA-TA (1000BaseT) Gigabit Ethernet device.<br>• Fixes the following DE600/DE602 10/100 Ethernet adapters problems:<br>– The primary CPU may appear hung on networks where switches send Flow Control Pause frames if they become overloaded.<br>– Transmit timeout messages appearing in the console log due to the driver timing out a frame.<br>• Updates the emx Fiber Channel driver to revision 1.21 which corrects a Data Error that is seen when running with the latest Emulex firmware. This error corrupts data when reading from the disk. |

**Table 2–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 285.00<br>OSF500X11-019 | **Patch:** X server support for PCI to Ethernet/Graphics adapter<br>**State:** Supersedes patches OSF500X11-001 (36.00), OSF500X11-010 (58.00), OSF500X11-016 (283.00)<br>This patch corrects the following:<br>• Fixes a problem where, on systems with a Powerstorm 4D10T (ELSA Gloria Synergy) graphics board, sometimes the X server does not draw lines correctly.<br>• Provides the X server support for the PCI To Ethernet/Graphics Combo Adapter (3X-DEPVD-AA) (also known as the ITI6021E Fast Ethernet NIC 3D Video Combination Adapter, InterServer Combo, or JIB).<br>• Fixes a problem where, on systems with a PowerStorm 4D10T (ELSA Gloria Synergy, SN-PBXGK-BB) graphics card or a PCI To Ethernet/Graphics Combo Adapter (3X-DEPVD-AA), sometimes lines and images are not drawn correctly in scrolled windows.<br>• Fixes synchronization and drawing problems in the X server for the PowerStorm 4D10T (ELSA Gloria Synergy, SN-PBXGK-BB) graphics card. |
| Patch 288.00<br>OSF500CDE-014 | **Patch:** Fix for dtlogin<br>**State:** New. Supersedes patches OSF500CDE-013 (286.00)<br>This patch corrects the following:<br>• Fixes a problem where the Common Desktop Environment (CDE) login daemon, dtlogin, core dumps occasionally when servicing requests from XDMCP clients such as X terminals or PCs running X servers.<br>• Fixes a problem with the Common Desktop Environment (CDE) login process where, if you selected the Command Line Login option and logged in, sometimes the CDE login screen would be redisplayed before you had logged out. |

**Table 2–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 299.00<br>OSF500DX-010 | **Patch:** Fixes problem with duplicate user identifier (UID)<br>**State:** Supersedes patches OSF500DX-006 (57.00), OSF500DX-001 (34.00), OSF500DX-002 (35.00), OSF500DX-004 (55.00), OSF500DX-018 (289.00), OSF500DX-013 (290.00), OSF500DX-017 (291.00), OSF500DX-016 (292.00), OSF500DX-009 (293.00), OSF500DX-015 (294.00), OSF500DX-019 (295.00), OSF500DX-008 (296.00), OSF500DX-022 (297.00)<br>This patch corrects the following:<br>• Fixes a situation in which a system running dxaccounts under C2 security mode experiences problems with a core dump when a user attemps to lock a retired user account.<br>• Fixes the problem with the useradd, usermod, and userdel commands, removing the last entry of the /etc/passwd file when the last line of the /etc/passwd file does not end with the new line character (\n).<br>• Fixes a problem in which the command usermod was not allowing any commas in the comment field when the current GECOS fields are filled.<br>• Fixes a problem in which duplicate user identifier (UID) is accepted at a second attempt even if the no duplicate user identifier policy is set.<br>• Fixes the following two problems existing in the cli command useradd:<br>– When running useradd X and useradd Y on the same machine but from separate terminals, two different type of contention error message are displayed.<br>– The following commands does not display an error message, which it should, when executed from a NIS clent:<br>usermod (or useradd) -x local=0<br>groupmod (or groupadd) -x local=0<br>• Fixes a situation in which a system running ASU experiences dxaccounts crash problem when a user is deleted from PC User view.<br>• Fixes the following problems of a dxaccounts application on ASU systems:<br>– dxaccounts crashes when the root icon is double clicked.<br>– The fullname of a new PC account is not mapped to a UNIX user.<br>– Erasing a PC account's fields does not work: the values erased remains.<br>– The default values of Home Directory, Login Script, and User Profile Path for a PC user are invalid.<br>• Fixes the problem of enabling to change root's login/uid through cli/dxaccounts utilities.<br>• Fixes the problem of not setting c2 security attributes values when useradd/usermod commands with -x account_inactive \| account_expiration are executed.<br>• Fixes a dxaccounts problem which prevents creating a new user from the PC Users view on a system with ASU installed. |

**Table 2–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 299.00 continued | • Fixes the problem of -t flag in useradd and usermod commands' usage.<br>• Fixes the problem of incorrect results from the command usermod -G.<br>• Fixes a problem where the new home directory for a new user ID is created with the date and time stamp of the /usr/skel directory.<br>• Fixes the problem of dxaccounts dialog messages incorrectly displayed when a user is added with no password entry. |
| Patch 301.00<br>OSF500-230A | **Patch:** Fix for incorrect timestamp display<br>**State:** New<br>evmshow and the event viewer display incorrect timestamps for binlog events on some Alpha EV6 systems. |
| Patch 303.00<br>OSF500-230B | **Patch:** Fix for evmshow<br>**State:** New<br>evmshow and the event viewer display incorrect timestamps for binlog events on some Alpha EV6 systems. |
| Patch 305.00<br>OSF500-201 | **Patch:** Fix for ITPSA driver<br>**State:** Supersedes patches OSF500-002 (1.00), OSF500-104 (68.00)<br>This patch corrects the following problems on the KZPCM and 8952U adapters:<br>• A panic, machine check, or hang can occur when aborting an I/O due to a command timeout or aborting an application program with pending I/Os.<br>• Fixes problems related to the ITPSA driver where errors can occur while the system is processing a SCSI bus or SCSI bus device reset request that is issued.<br>• Includes a fix to a problem on the 8951U and 8952U adapters. SCSI bus resets are lost when these adapters are connected to single ended drives.<br>• Fixes a lockmode 4 panic on boot.<br>• Fixes a problem where chip interrupt register fields in error log are incorrect.<br>• Fixes that lessen the opportunity of aborts being issued for an already completed I/O.<br>• Fixes kernel memory fault panic caused by a SWS data structure being released twice.<br>• Fixes a simple lock timeout panic. It was possible for a bus reset to be generated before the previous bus reset was processed causing excessive processing within the ISR.<br>• Fixes a problem with the ITPSA driver. The driver negotiated for ULTRA2 speed when it was attached to a single-ended bus.<br>• Fixes a problem with ITPSA driver in which the system will panic in itpsa_allocReq() on boot when lockmode=4 is set. |

**Table 2–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 311.00<br>OSF500-301 | **Patch:** Various print fixes<br>**State:** New. Supersedes patches OSF500-164 (306.00), OSF500-256 (307.00), OSF500-264 (308.00), OSF500-185 (309.00)<br>This patch corrects the following:<br>• When using the I18N ya option, the queue daemon filters will terminate after 32 jobs.<br>• Under certain circumstances, print jobs are terminated when printing to certain printers that are connected to a DECserver through TCP/IP.<br>• Fixes a printing problem where lpd reads any data from the printer that has not been read for local and remote connections. The read-backs for remote connections cause an additional 2 second timeout which may cause a job-submit failure on the job-number wraparound.<br>• A user is unable to delete a print job from a remote system with a hostname greater than 32 characters because the hostname was truncated.<br>• When a TCP/IP connection fails, the retry algorithm would take longer to print jobs due to a long retry interval.<br>• A timing hole during lpd last-job completion and shutdown needed to be closed.<br>• It was not possible to print to the lpd queue using Windows 2000.<br>• The lprm command does not kill lpd when the currently running job is specified.<br>• Remote print jobs set root:daemon as owner. This is incorrect, and causes jobs to be lost.<br>• Corrects a problem in which, under certain conditions, unnecessary error messages are written to the lpr.log file. |
| Patch 313.00<br>OSF500-174 | **Patch:** Fix for tftpd problem<br>**State:** New<br>This patch fixes a tftpd problem when responding to a broadcast read request and it adds the -b option to control whether to respond to any braodscasts. |
| Patch 315.00<br>OSF500-202 | **Patch:** Fix for restore command<br>**State:** New<br>This patch fixes a problem in which the restore command can fail with the following error:<br>Cannot malloc space for property list |
| Patch 317.00<br>OSF500-202 | **Patch:** Fix for collect information tool<br>**State:** Supersedes patches OSF500-114 (77.00)<br>This patch fixes the following two problems with the collect information tool used by the sys_check utility:<br>• A security hole where a user can become root.<br>• collect can not start at boot time due to incorrectly handling SIGHUP signal.<br>• Fixes several problems with the collect command and adds sysloging when collect suspends, resumes, or receives a signal. |
| Patch 319.00<br>OSF500DX-007 | **Patch:** Problem when Sysman processes NFS configuration<br>**State:** New<br>This patch fixes problems that occur when Sysman processes NFS configuration parameters in the /etc/rc.config files. |

**Table 2–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 321.00<br>OSF500-192 | **Patch:** Fix for verify command<br>**State:** New<br>This patch fixes a problem with verify where verify fails to complete on systems with a large number of files. |
| Patch 323.00<br>OSF500X11-025A | **Patch:** Fix for toggle button problem<br>**State:** Supersedes patches OSF500X11-005A (59.00), OSF500X11-009A (63.00)<br>This patch corrects the following:<br>• Fixes a problem with the toggle button where if a display is closed and reopened then the X Server may generate an "Invalid Pixmap Error".<br>• Fixes a problem with the Motif libraries where sometimes widgets or windows were created with the wrong size (XmNwidth and XmNheight were very small).<br>• Fixes various memory leaks in the Motif library (libXm) that could occur when creating and destroying Motif List, Text, and TextField widgets. |
| Patch 325.00<br>OSF500X11-025B | **Patch:** X server generates Invalid Pixmap Error<br>**State:** Supersedes patches OSF500X11-005B (145.00), OSF500X11-009B (147.00)<br>This patch corrects the following:<br>• Fixes a problem with the toggle button where if a display is closed and reopened then the X Server may generate an "Invalid Pixmap Error".<br>• Fixes a problem with the Motif libraries where sometimes widgets or windows were created with the wrong size (XmNwidth and XmNheight were very small).<br>• Fixes various memory leaks in the Motif library (libXm) that could occur when creating and destroying Motif List, Text, and TextField widgets. |
| Patch 327.00<br>OSF500CDE-009 | **Patch:** Adds ISO8859-15 functionality to Xresource file<br>**State:** Supersedes patches OSF500CDE-006 (53.00)<br>This patch adds the ISO8859-15 functionality to the main Xresource file on the system and to the specific dtlogin resource file. With these changes, X applications to have ISO8859-15 locale support integrated directly into the application. This patch adds Catalan (ISO8859-15) to the list of languages from which users can choose when logging in. The additional item identifies the Catalan Latin-9 locale, which supports the Euro currency sign. |
| Patch 329.00<br>OSF500-218 | **Patch:** C shell causes segmentation fault<br>**State:** Supersedes patches OSF500-020 (19.00), OSF500-076 (122.00)<br>This patch corrects the following:<br>• Corrects how the C shell handles 2-byte characters when running in the Japanese SJIS locale.<br>• Fixes a problem in the C shell (csh) in which a segmentation fault will occur when the user defines an environmental variable which exceeds the 2048 character limitation. This limit has been lengthened to 8192 characters.<br>• Fixes a C shell problem where multibyte characters may not be displayed properly inside quotes. |

**Table 2–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 331.00<br>OSF500-254 | **Patch:** Fix for advscan<br>**State:** New<br>This patch fixes a problem where advscan -a -g does not display bootable partitions properly. |
| Patch 333.00<br>OSF500-249 | **Patch:** Fix for salvage command<br>**State:** New<br>This patch corrects the following:<br>• Fixes two infinite loops that could make salvage run forever.<br>• Salvage could core dump when encountering a deleted property list. |
| Patch 335.00<br>OSF500CDE-010A | **Patch:** Security (SSRT0617U)<br>**State:** New<br>A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability. |
| Patch 337.00<br>OSF500CDE-010B | **Patch:** Security (SSRT0617U)<br>**State:** New<br>A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability. |
| Patch 339.00<br>OSF500-282 | **Patch:** Fix for what command<br>**State:** New<br>The what command was unable to process more than one input file at once. |
| Patch 341.00<br>OSF500-266 | **Patch:** Security (SSRT0683U)<br>**State:** New<br>A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability. |

**Table 2–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 344.00<br>OSF500-291 | **Patch:** Fix for Compaq C compiler<br>**State:** Supersedes patches OSF500-036 (29.00), OSF500-127 (90.00), OSF500-215 (342.00)<br>This patch fixes the following problems in the Compaq C compiler:<br>• A compile-time performance problem with a very large (1.6 MB) array initialization.<br>• A compiler crash when compiling intrinsic memset.<br>• A run-time error for a program containing an unsigned long in a for loop and is compiled -arch ev6 -O.<br>• A compiler crash when using cc -feedback.<br>• A run-time error for a program involving the incorrect evaluation of temp = w*(iter+1); in a while loop.<br>• A run-time error for a program containing k = (char)(l >> 8) is not sign-extended when compiled using -O.<br>• A compiler crash when duplicate function prototypes found in function scope.<br>• A compiler crash when using the -MD flag to generate dependency files in a non-writable directory.<br>• A compiler crash when compiling Xemacs 21.1.4 with -O4.<br>• An optimizer problem in loop unrolling that suppressed intermediate updates to induction variables under certain conditions.<br>• A potential problem with scheduling and .arch ev6 when producing assembly files using -S.<br>• An optimizer problem that produced incorrect code when certain bounds checking within a loop was moved outside the loop.<br>• A virtual memory exhausted error when compiling the Open Source encryption library OpenSSL.<br>• An optimizer problem in loop unrolling that caused an incorrect result under certain conditions.<br>• Various compiler crashes under certain conditions.<br>• An optimizer problem that caused some of the exception handling example programs in Chapter 11 of the Programmer's Guide to fail.<br>• An optimizer problem that caused a Perl validity test to fail when using a long double NaN.<br>• An optimizer problem that caused the wrong answer to be produced for a program involving tail recursion. |
| Patch 347.00<br>OSF500-286 | **Patch:** Fix for mv command<br>**State:** New. Supersedes patches OSF500-277 (345.00)<br>This patch corrects the problem with the mv(1) command deleting files in the directory when the user moves a directory to itself. |
| Patch 349.00<br>OSF500-195 | **Patch:** Invalid msgs appear in daemon.log<br>**State:** New<br>This patch prevents the message "nfscast: select: Invalid argument" message from appearing in the daemon.log when the server is not available. It also changes the "trymany: servers not responding: RPC: Unable to receive" message to an informational versus an error message. |

**Table 2–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 351.00<br>OSF500-160 | **Patch:** Fix for vi, ex, and more commands<br>**State:** New<br>This patch corrects the error handling when invalid multibyte sequences are encountered by the vi, ex, or more commands. |
| Patch 353.00<br>OSF500-189 | **Patch:** quotactl prototype now meets POSIX standards<br>**State:** New<br>This patch is to change the quotactl prototype in /usr/include/ufs/quota.h to meet POSIX standards. |
| Patch 355.00<br>OSF500-246 | **Patch:** Fix for encoding problem with audit<br>**State:** New<br>This patch fixes a problem where encoding for the SysV Open call audit parameter was incorrect. This could cause a system panic. |
| Patch 357.00<br>OSF500-168 | **Patch:** Fixes DE500 interfaces using Micro Linear ML6694F PHY<br>**State:** New<br>This patch corrects a problem with some DE500 interfaces that use the Micro Linear ML6694F PHY. |
| Patch 359.00<br>OSF500-292 | **Patch:** Upgrades sys_check utility to Version 119.1<br>**State:** New<br>This patch upgrades sys_check utility to Version 119.1 and provides the following changes:<br>• Two NFS bugs.<br>• Utilizes Compaq Analyze when available.<br>• Utilizes storage's new cliscript tool in place of hszterm.<br>• Updated ASU section. |
| Patch 361.00<br>OSF500DX-011 | **Patch:** Fix for CDE setup application<br>**State:** New<br>This patch fixes the problem where the CDE setup Application does not come up when invoked from unicode locales if localized setup files do not exist.This patch adds error detection when no localized setup files exist. |
| Patch 363.00<br>OSF500DX-023 | **Patch:** Fix for diskconfig<br>**State:** New<br>This fixes a problem that was causing diskconfig to issue the error message "can't read tminor: no such variable" upon startup. |
| Patch 365.00<br>OSF500CDE-011 | **Patch:** Fix for CDE application manager<br>**State:** New<br>This patch fixes a problem where the Common Desktop Environment (CDE) Application Manager did not recreate the list of application groups at login. After customizing the application groups, users would see the old groups instead of the new groups. |
| Patch 367.00<br>OSF500-183 | **Patch:** Fixes a hang in the shutdown process<br>**State:** New<br>This patch fixes a hang in the shutdown process (shutdown now) of a system when a device has flow control switched off. |

**Table 2–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 369.00<br>OSF500-147 | **Patch:** Fixes various AdvFS problems<br>**State:** New<br>This patch fixes the following AdvFS problems:<br>• The mount_advfs utility will core dump upon a return error of ENODEV from the kernel.<br>• When a valid AdvFS domain has a corrupted pointer to a domain volume, a ENODEV error is returned, but is incorrectly reported as an E_ADVFS_NOT _INSTALLED error. |
| Patch 371.00<br>OSF500-146 | **Patch:** Fix for SCU command<br>**State:** New<br>This patch fixes the following problems:<br>• Processes may hang due to waiting for I/O interrupts.<br>• The SCU command set pages pcf will hang a system when ATAPI CDrom device is selected. |
| Patch 373.00<br>OSF500-171 | **Patch:** Fix for comsat daemon core dump problem<br>**State:** New<br>This patch fixes a problem where the comsat daemon core dumps each time it receives reports of incoming mail and notifies users who request this service. |
| Patch 375.00<br>OSF500-213 | **Patch:** Fix for sort command<br>**State:** Supersedes patches OSF500-023 (22.00), OSF500-122 (85.00)<br>This patch corrects the following:<br>• Fixes a problem in which sort -i a_file >b_file aborts with the message "A line of the input file contains more than 20480 characters" when LANG = da_DK.ISO8859-1.<br>• Fixes a problem in which the sort command aborts with the message "A line of the input file contains more than 20480 characters" when running in a Japanese locale.<br>• Fixes a problem that sometimes occurs when sorting large data files in a multibyte locales such as Japanese. |
| Patch 377.00<br>OSF500-158 | **Patch:** UFS disk quotas do not automatically update<br>**State:** New<br>This patch fixes a problem where UFS disk quota's are not updating automatically. |
| Patch 379.00<br>OSF500X11-024A | **Patch:** Fix for memory leak in the X Toolkit library<br>**State:** Supersedes patches OSF500X11-007A (61.00)<br>This patch corrects the following:<br>• Fixes a memory leak in the X Toolkit library (libXt). This memory leak could be seen by applications that create and destroy many Motif ScrolledWindow widgets.<br>• Fixes a memory leak in the X Window System's X Toolkit library (Xt) that could occur when creating and destroying Motif List, Text, and TextField widgets. |

**Table 2–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 381.00<br>OSF500X11-024B | **Patch:** Fix for memory leak in the X Toolkit library<br>**State:** Supersedes patches OSF500X11-007A (61.00)<br>This patch corrects the following:<br>• Fixes a memory leak in the X Toolkit library (libXt). This memory leak could be seen by applications that create and destroy many Motif ScrolledWindow widgets.<br>• Fixes a memory leak in the X Window System's X Toolkit library (Xt) that could occur when creating and destroying Motif List, Text, and TextField widgets. |
| Patch 383.00<br>OSF500-247 | **Patch:** Fix for snmpd<br>**State:** New<br>This patch fixes a problem where snmpd sends SNMPv1 trap messages with an internal address field ==0. |
| Patch 385.00<br>OSF500-223 | **Patch:** Fix for simple lock panic<br>**State:** New<br>This patch fixes a problem in which the system may panic with the error message "simple lock: time limit exceeded" when running ATM. |
| Patch 388.00<br>OSF500X11-015 | **Patch:** Fix for libDXm.so svn widget<br>**State:** New. Supersedes patches OSF500X11-011A (386.00)<br>This patch corrects the following:<br>• Fixes a problem in which the svn widget of libDXm.so creates identical backgrounds and foregrounds.<br>• Fixes a problem where the acl settings are lost when they are changed by using the GUI dxsetacl command. |
| Patch 390.00<br>OSF500X11-011B | **Patch:** libDXm static library fix<br>**State:** New<br>This patch fixes a problem in which the svn widget of libDXm.so creates identical backgrounds and foregrounds. |
| Patch 392.00<br>OSF500-190 | **Patch:** Various fixes for ld command<br>**State:** Supersedes patches OSF500-012 (11.00), OSF500-105 (69.00), OSF500-116A (79.00)<br>This patch corrects the following:<br>• Fixes a problem where the linker (ld) would insert incorrect values for the symbols etext and _etext when building kernels larger than 4 MB.<br>• Fixes a problem where the linker (ld) could not read arguments longer than 1024 characters in input files. This also adds proper support for line continuation characters.<br>• Fixes a problem where the linker and OM would not properly process a large (multi-GOT) image in the presence of the -om option. This patch also fixes a problem with the linker not properly handling scTlsUndefined symbols.<br>• Including a shared library on a link line twice with another library in between caused unresolved symbols in some cases.<br>• Linking large applications with -om -call_shared with very large numbers of external symbols sometimes failed to link. |

**Table 2–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 394.00<br>OSF500-141 | **Patch:** Fix for defragment program<br>**State:** Supersedes patches OSF500-081 (126.00)<br>This patch corrects the following:<br>• Fixes the defragment program to properly report on extremely large (>4.3GB) freespace holes. Previously it would report Free space percentages larger than 100% and would add these large holes to the smallest range (<100K) instead of the largest range (>10M) where they belong.<br>• Fixes a problem in which defragment reports incorrect extent counts on files with a large number of extents. |
| Patch 396.00<br>OSF500-244 | **Patch:** Fix for CPU hang<br>**State:** New<br>This patch fixes a kernel panic seen when running Classical IP over the lfa ATM driver. This panic would only occur in lockmode 4. If not in lockmode 4, the symptom would be a CPU hang. |
| Patch 399.00<br>OSF500-178 | **Patch:** Fix for problem that occurs when creating ATM ELANs<br>**State:** Supersedes patches OSF500-019 (18.00), OSF500-248 (397.00)<br>This patch corrects the following:<br>• Fixes a problem with the creation of multiple ATM ELANS. When running ATM Lan Emulation, using more than four ATM NetRAIN interfaces can result in recursive calls causing a kernel stack not valid halt.<br>• Fixes a problem in which the system may panic with the error message "Unaligned kernel space access from kernel mode" when running ATM ELANs. |
| Patch 401.00<br>OSF500-273 | **Patch:** Fix for vdump program dumping core<br>**State:** Supersedes patches OSF500-044 (33.00)<br>This patch corrects the following:<br>• The vdump program would dump core with the following message:<br>nnnn Resources lost(coredump)<br>• Fixes a problem where the vdump command will sometimes store symbolic link files as directories in the vdump archive. |
| Patch 405.00<br>OSF500X11-012A | **Patch:** Fix for Xlib memory leaks<br>**State:** New. Supersedes patches OSF500X11-023A (402.00), OSF500X11-017 (403.00)<br>This patch corrects the following:<br>• Fixes two memory leaks in the X Window System's X library (Xlib) that can occur when creating and destroying Motif List, Text, and TextField widgets.<br>• Fixes a problem in which some 8-bit characters cannot be entered directly from the keyboard when the Caps Lock setting is on.<br>• Fixes a problem where font selection in dtterm produces a corrupted output for LATIN-2 locales. |
| Patch 408.00<br>OSF500X11-012B | **Patch:** Fix for memory leaks<br>**State:** New. Supersedes patches OSF500X11-023B (406.00)<br>This patch corrects the following:<br>• Fixes two memory leaks in the X Window System's X library (Xlib) that can occur when creating and destroying Motif List, Text, and TextField widgets.<br>• Fixes a problem where font selection in dtterm produces a corrupted output for LATIN-2 locales. |

**Table 2–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 410.00<br>OSF500-287 | **Patch:** Fix for bootlink failure<br>**State:** New<br>This patch fixes a problem in which the bootlink can fail on AlphaStations 600, 600A, and 500/400. |
| Patch 412.00<br>OSF500-212 | **Patch:** Update for Danish locale<br>**State:** New<br>This patch updates the Danish (da_DK.ISO8859-1) locale to use all lowercase month names. |
| Patch 414.00<br>OSF500-154 | **Patch:** Security (SSRT0624U)<br>**State:** New<br>A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability. |
| Patch 416.00<br>OSF500X11-018 | **Patch:** Fix for lbxproxy utility<br>**State:** New<br>This patch fixes a problem where the X windows lbxproxy utility, which is used to make Low Bandwidth X (LBX) connections to an X server, did not accept local connections. |
| Patch 418.00<br>OSF500-188 | **Patch:** Updates lfa ATM driver to V1.0.16<br>**State:** Supersedes patches OSF500-058 (107.00)<br>This patch corrects the following:<br>• Updates the lfa ATM driver to V1.0.16 and fixes the following two ATM driver problems:<br>– Fixes a soft hang that can occur when running NFS over ATM.<br>– Allows the ATM subsystem to be shut down successfully in the event of a board hang.<br>• Updates the lfa ATM device driver to V1.0.17 and adds some enhancements as well as a fix for a kernel memory fault seen when either shutting down or restarting the device driver. |
| Patch 422.00<br>OSF500-136 | **Patch:** Security (SSRT0642U)<br>**State:** Supersedes patches OSF500-099 (144.00), OSF500-177 (419.00), OSF500-275 (420.00)<br>This patch corrects the following:<br>• A potential security vulnerability has been discovered, where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability.<br>• Corrects a “permission denied” error when writing to the /var/tcb/files/dblogs/[logfile] while running pop3d and enhanced security.<br>• Fixes a problem for Enhanced Security configurations where the Maximum Login Interval (u_max_login_intvl) field was being ignored for account templates.<br>• Corrects a problem of the rsh command displaying a warning message instead of the rsh command output when C2 security is configured. |

**Table 2–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 424.00<br>OSF500DX-020 | **Patch:** SNMP subagent core dumps at boot up time<br>**State:** New<br>This patch fixes a problem that causes Compaq SNMP subagent (cpq_mibs) to coredump at boot-up time or when being reinvoked, which results in invalid display of information on Insight Manager web pages. |
| Patch 426.00<br>OSF500X11-020A | **Patch:** Security (SSRT0656U)<br>**State:** New<br>A potential security vulnerability has been discovered, where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability. |
| Patch 428.00<br>OSF500X11-020B | **Patch:** Security (SSRT0656U)<br>**State:** New<br>A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability. |
| Patch 430.00<br>OSF500-207 | **Patch:** Fixes various problems with om<br>**State:** Supersedes patches OSF500-115 (78.00), OSF500-116B (148.00)<br>This patch corrects the following:<br>• Fixes various problems with om (/usr/lib/cmplrs/om).<br>• Fixes a problem where the linker and om would not properly process a large (multi-GOT) image in the presence of the -om option. This patch also fixes a problem with the linker not properly handling scTlsUndefined symbols.<br>• Fixes three errors that are occasionally seen when compiling with the -om switch:<br>om: fast access range error<br>om: value(0x1201704de) not in range of GP table<br>core dumping in the routine reloc_abs() |
| Patch 432.00<br>OSF500-259 | **Patch:** Fixes a panic in cdfs<br>**State:** Supersedes patches OSF500-108 (72.00), OSF500-057 (106.00), OSF500-095 (140.00)<br>This patch corrects the following:<br>• Fixes a problem where the system can panic with the panic string "secsize_resid < d_reclen" when accessing a defective CDROM.<br>• Fixes a problem in which system may memory fault if CFS server no longer had access to the CDROM device.<br>• Fixes a panic in cdfs that has the following error message:<br>Panic: simple_unlock: no locks owned by cpu; vnode.v_lock class<br>• Fixes a problem with cdfs. Fatal errors occur when trying to load data from a cdfs CDROM over NFS. |
| Patch 434.00<br>OSF500CDE-012 | **Patch:** Fix for dtmail problem<br>**State:** New<br>This patch fixes a dtmail problem in which a From line with quotes in it incorrectly finds the date of the mail message. This error is displayed on the main screen under the header Date and Time and shows up as Dec. 31 or as a blank field. |

**Table 2–2: Summary of Base Operating System Patches (cont.)**

| | |
|---|---|
| Patch 437.00<br>OSF500-325 | **Patch:** Floppy driver fix<br>**State:** New. Supersedes patches OSF500-187 (435.00)<br>Compaq has determined in laboratory testing that there is a theoretical possibility that during read and write operations to the floppy disk on DS10, DS10L and ES40 AlphaServers and VS10 and XP900 AlphaStations, a single byte of data may be inaccurately read or written without notice to the user or system. The potential for this anomaly exists only if floppy data read and write operations are attempted while there is extremely heavy traffic on these Alpha systems' internal input/output busses. Although Compaq has observed the anomaly only in laboratory tests designed to create atypical system stresses, including almost constant use of the floppy disk drive, we are supplying this patch to address this potential issue. |
| Patch 439.00<br>OSF500CDE-015 | **Patch:** dtwm intermittently hangs<br>**State:** New<br>This patch fixes a problem in which the Window Manager (dtwm) intermittently hangs on a system which uses multiple displays. |
| Patch 442.00<br>OSF500-267 | **Patch:** crontab jobs run multiple times in same minute<br>**State:** New. Supersedes patches OSF500-226 (440.00)<br>This patch corrects the following:<br>• Fixes a problem where some crontab jobs would run multiple times in the same minute.<br>• Fixes two cron problems:<br>– The cron daemon does intensive logging and fills up the disk.<br>– Multiple cron daemons continue to run and consume system resources due to the fact that, after a user is deleted from the system, there are still jobs running on the users behalf. |