DIGITAL UNIX 4.0E and TruCluster 1.5

Patch Summary and Release Notes Patch Kit-0004

March 2000

This manual describes the release notes and contents of Patch Kit-0004. It provides any special instructions for installing individual patches.

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

Compaq Computer Corporation
Houston, Texas

Contents

About This Manual

This manual contains information specific to Patch Kit-0004 for the DIGITAL UNIX Version 4.0E operating system and TruCluster 1.5 software products. It provides a list of the patches contained in each kit and describes any information you need to know when 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.

Chapter 3 Summarizes the TruCluster software 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 DIGITAL UNIX and TruCluster documents:

- DIGITAL UNIX, ASE, and TCR *Patch Kit Installation Instructions*
- DIGITAL UNIX *Installation Guide*
- DIGITAL UNIX *System Administration*
- TruCluster Software Products *Software Installation*
- TruCluster Software Products *Administration*
- Any release-specific installation documentation

Reader's Comments

Compaq welcomes any comments and suggestions you have on this and other DIGITAL 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 DIGITAL UNIX that you are using.
- If known, the type of processor that is running the DIGITAL UNIX software.

The DIGITAL 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 DIGITAL UNIX 4.0E and TCR 1.5 Patch Kit-0004.

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 ~41.0 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 ~41.9 MB of storage space in /var/adm/patch may be required for original files if you choose to install and revert all patches. See the *Patch Kit Installation Instructions* for more information.

  Up to ~653 KB of storage space is required in /var/adm/patch/doc for patch abstract and README documentation.

  A total of ~128 KB of storage space is needed in /usr/sbin/dupatch for the patch management utility.

TruCluster Software products

- 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 ~46.5 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 ~47.3 MB of storage space in /var/adm/patch may be required for original files if you choose to install and revert all patches. See the *Patch Kit Installation Instructions* for more information.

  Up to ~732 KB of storage space is required in /var/adm/patch/doc for patch abstract and README documentation.

  A total of ~128 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 Notes for Patch 590.00

This patch provides the following new features for bootable tape.

The updated btcreate(8) reference page sections follow:

- Using the -d option, a user can choose the location where the btcreate command creates its temporary files.

  Previously, btcreate was used to create its temporary files in the /usr filesystem and required about 156000 blocks (512 bytes per block) of disk space in the/usr filesystem. Now the user has the option of using free disk space anywhere on the system.

  In the following example, the temporary files will be created at /mnt/bt_tmp:

  ```
  # ./btcreate -d /mnt/bt_tmp
  ```

Note that the `btcreate -d` option has also been incorporated in the interactive mode.

- The ability for a user to label disks using their own `disklabel` script.

  If the customized `disklabel` script is not present, the `btextract` command will label the disks in the usual manner.

  A customized `disklabel` script has the following restrictions:

  – It must be located in the `/usr/lib/sabt/etc` directory.

  – It must be named `custom_disklabel_file`.

1.4 Release Notes for Patch 464.00

The following sections contain reference page updates.

1.4.1 Reference Page Update for cron(8)

1. Add the following to the DESCRIPTION section:

   When the `cron` daemon is started with the `-d` option, a trace of all jobs executed by `cron` is output to file `/var/adm/cron/log`.

2. Add the following to the FILES section:

   ```
   /var/adm/cron/cron.deny
     List of denied users
   /var/adm/cron/log
     History information for cron
   /var/adm/cron/queuedefs
     Queue description file for at, batch, and cron
   ```

3. Add `queuedefs(4)` to the Files: section of RELATED INFORMATION.

1.4.2 New Reference Page for queuedefs(4):

queuedefs(4) queuedefs(4)

NAME

queuedefs - Queue description file for at, batch, and cron commands

DESCRIPTION

The queuedefs file describes the characteristics of the queues managed by cron or specifies other characteristics for cron. Each noncomment line in this file describes either one queue or a cron characteristic. Each uncommented line should be in one of the following formats.

```
q.[njobj][nicen][nwaitw]
max_jobs=mjobs
log=lcode
```

The fields in these line are as follows:

q The name of the queue. Defined queues are as follows:

a The default queue for jobs started by at

b The default queue for jobs started by batch

c The default queue for jobs run from a crontab file

Queues d to z are also available for local use.

njob The maximum number of jobs that can be run simultaneously in the queue; if more than njob jobs are ready to run, only the first njob jobs will be run. The others will be initiated as currently running

jobs terminate.

nice The nice(1) value to give to all jobs in the queue that are not run with a user ID of superuser.

nwait The number of seconds to wait before rescheduling a job that was deferred because more than njob jobs were running in that queue, or because the system-wide limit of jobs executing (max_jobs) has been reached.

mjobs The maximum number of active jobs from all queues that may run at any one time. The default is 25 jobs.

lcode Logging level of messages sent to a log file. The default is 4. Defined levels are as follows:

level-code level

0 None

1 Low

2 Medium

3 High

4 Full

Lines beginning with # are comments, and are ignored.

EXAMPLES

The following file specifies that the b queue, for batch jobs, can have up to 50 jobs running simultaneously; that those jobs will be run with a nice value of 20. If a job cannot be run because too many other jobs are running, cron will wait 60 seconds before trying again to run it. All other queues can have up to 100 jobs running simultaneously; they will be run with a nice value of 2, and if a job cannot be run because too many other jobs are running, cron will wait 60 seconds before trying again to run it.

```
b.50j20n60w
```

The following file specifies that a total of 25 active jobs will be allowed by cron over all the queues at any one time, and cron will log all messages to the log file. The last two lines are comments that are ignored.

```
max_jobs=25
log=4
# This is a comment
# And so is this
```

FILES

/var/adm/cron
Main cron directory

/var/adm/cron/queuedefs
The default location for the queue description file.

RELATED INFORMATION

Commands: at(1), cron(8), crontab(1), nice(1)

1.4.3 Reference Page Update for crontab(1):

On days when the daylight saving time (DST) changes, cron schedules commands differently from normal.

The two rules described below specify cron's scheduling policy for days when the DST changes. First some terms will be defined.

An AMBIGUOUS time refers to a clock time that occurs twice
in the same day because of a DST change (usually on a day during Fall).

A NONEXISTENT time refers to a clock time that does not occur
because of a DST change (usually on a day during Spring).

DSTSHIFT refers to the offset that is applied to standard time to
result in daylight savings time. This is normally one hour, but can be
any amount of time up to 23 hours and 59 minutes.

The TRANSITION period starts at the first second after the DST shift
occurs, and ends just before DSTSHIFT time later.

An HOURLY command has a * in the hour field of the crontab entry.

RULE 1: (AMBIGUOUS times)

A nonhourly command is run only once at the first occurrence
of an ambiguous clock time.

- A non-hourly command scheduled for 01:15 and 01:17
  will be run at 01:15 and 01:17 EDT on 10/25/98
  and will not be run at 01:15 or 01:17 EST.

An hourly command is run at all occurrences of an ambiguous time.

- An hourly command scheduled for *:15 and *:17
  will be run at 01:15 and 01:17 EDT on 10/25/98
  and also at 01:15 and 01:17 EST.

RULE 2: (NONEXISTENT times)

A command is run DSTSHIFT time after a nonexistent clock time.

If the command is already scheduled to run at the newly shifted time,
then the command is run only once at that clock time.

- A nonhourly command scheduled for 02:15 and 03:15
  will be run once at 03:15 EDT on 4/5/98.

- A nonhourly command scheduled for 02:15 and 02:17
  will be run once at 03:15 and once at 03:17 EDT on 4/5/98.

- An hourly command scheduled for *:15 and *:17
  will be run once at 03:15 and once at 03:17 EDT on 4/5/98.

Note:
cron's behavior during the transition period is undefined if the
DST shift crosses a day boundary, for example when the DST shift
is 23:29:29->00:30:00 and the transition period is 00:30:00->01:29:59.

Here are sample DST change values (for Eastern US time EST/EDT).
During the transition period, clock time may be either
nonexistent (02:00-02:59 EST in Spring)
or ambiguous (01:00-01:59 EDT or EST in Fall).

Spring (April 5, 1998):
  DST shift: 01:59:59 EST –> 03:00:00 EDT
  transition period: 03:00:00 EDT –> 03:59:59 EDT
  DSTSHIFT: 1 hour forwards

Fall (Oct 25, 1998):
  DST shift: 01:59:59 EDT –> 01:00:00 EST
  transition period: 01:00:00 EST –> 01:59:59 EST
  DSTSHIFT: 1 hour backwards

1.5 Release Notes for Patch 558.00

The updated reference page sections for lpr(1) follow:

The printer log, lpr.log now reports the creation of files preceded by a dot (.) in the spooling directories. Do not amend or delete these files as the printer subsystem manages their creation and cleanup.

For initial use, DIGITAL recommends that you set the logging level to lpr.info. If you have a problem that is escalated to technical support, the support organization will request lpr.log at the lpr.debug level. This is because the DEBUG messages provide a detailed trace that can only be interpreted by reference to the source code and lpr.log will simply grow more quickly if DEBUG messages are logged. The lpr.info level provides a shorter report of an event, including any network retry messages and unusual occurences (which are not always errors).

All changes to the status file of a queue, including reports of any files printed, are reported at the DEBUG level rather than the INFO level. This reduces the rate of growth of the file and allows you to monitor and react to important events more quickly. The WARNING level logs events that may need to be attended to, while the ERROR level logs hard (often fatal) errors.

To modify the logging level, edit your /etc/syslog.conf file and change the lpr line to the required level, such as lpr.info as follows:

```
lpr.info      /var/adm/syslog.dated
```

Use the ps command to find the PID for the syslog daemon, and the following command to re-start syslogd:

```
# kill -HUP
```

A new set of log files will be created in /var/adm/syslog.

As previously mentioned, this patch provides support to the BSD lpd(8) print system for Compaq's Advanced Printing Software (APX). This patch allows lpr(1) print jobs to be submitted to the Advanced Print System (APX).

1.6 Release Notes for Patches 534.00 and 321.00

This release notes describes enhanced performance for multithreaded applications for the malloc command.

To make optimum use of the malloc tuning features for performance–sensitive applications, the developer needs to consult the Tuning Memory Allocation section of the malloc(3) reference page.

In addition, three new tuning variables which are particularly important to multithreaded applications are added by this patch. They are described in the following sections.

1.6.1 int __delayed_free = 2;

The variable __delayed_free is used to cause the free() function to use a "delay slot" (of size one). This means that any time you call free, it saves your pointer and actually frees what you last called free with. This is intended to avoid misuse of realloc, where the user frees a pointer and then calls realloc with it. Since the delay slot is shared across all threads, this will not provide reliable protection for multithreaded applications. It also means that it is accessed internally with atomic instruction sequences which can create a bottleneck on multi-CPU systems.

A value of 1 means only delay frees for single-threaded applications. A value of 2 means delay for both single and multithreaded applications. A value of 0 turns this feature off for both classes of applications. All other values cause undefined behavior. It is recommended that all multithreaded applications try to use a value of 1. The default value of 2 will change to 1 in a future release.

1.6.2 int __first_fit = 0;

The variable `__first_fit` is currently intended only for performance–critical multithreaded applications. It should not be used with single-threaded applications. Its value is used to allow `malloc` and `amalloc` to skip up to a larger internal cache list if the optimum node size list is found to be in use by another thread. The allowed values are 0, 1, and 2. Do not use any other value.

A value of 0 disables this feature. A value of 1 allows the next larger list to be used, and a value of 2 allows the next list after that to also be used (three lists in total). Increasing the value of `__first_fit` can increase both execution speed and memory consumption of multithreaded applications making heavy concurrent use of either `malloc` functions or the same arena with `amalloc` functions.

1.6.3 int __max_cache = 15;

The `__max_cache` variable suggests the number of internal cache (lookaside) lists to be used by `malloc` and `amalloc`. Each list contains blocks within the same size range. A larger value of `__max_cache` causes the internal caching of larger sized blocks. The currently allowable values for this variable are 15, 18, 21, 24, and 27. Do not use any other value. The given values correspond to lists containing nodes up to 632, 1272, 2552, 5112, and 10232 bytes in size, respectively. The maximum length of the lists is determined by the `__fast_free_max` variable.

Application requests for storage that can be satisfied from a node on a cache list typically happen somewhat faster than those that cannot. Increasing the value of this variable can increase both the execution speed and the memory consumption of an application that allocates nodes in the given size range.

1.7 Release Notes for Patches 320.00 and 321.00

This release note contains the new reference page for `amalloc`(3).

A new set of memory allocator functions, collectively known as `arena malloc`, has been added in this patch. The reference page follows:

amalloc(3) amalloc(3)

NAME

acalloc, acreate, adelete, afree, amallinfo, amalloc, amallopt,
amallocblk-size, arealloc - arena memory allocator

LIBRARY

Standard C Library (libc.so, libc.a)

SYNOPSIS

```
#include  #include
void *acreate (
      void *addr, size_t len, int flags, void *ushdr,
      void *(*grow_func)(size_t, void *));
int adelete (void *ap);
void *amalloc (
      size_t size, void *ap);
void afree (
      void *ptr, void *ap);
```

```
void *arealloc (
      void *ptr, size_t size, void *ap);
void *acalloc (
      size_t nelem, size_t elsize, void *ap);
size_t amallocblksize (
      void *ptr, void *ap);
```

The following function definitions are provided only for System V compatibility:

```
int amallopt (
      int cmd, int value, void *ap);
struct mallinfo amallinfo (
      void *ap);
```

DESCRIPTION

The amalloc family of routines provides a main memory allocator based on the malloc(3) memory allocator. This allocator has been extended so that an arbitrary memory space ("arena") can be set up as an area from which to allocate memory.

Calls to the amalloc family of routines differ from calls to the standard malloc(3) only in that an arena pointer must be supplied. This arena pointer is returned by a call to acreate.

acreate
Sets up an area defined as starting at virtual address addr and extending for len bytes. Arenas can be either growing or nongrowing.

An arena that is nongrowing is constrained to use only up to len bytes of memory. The grow_func parameter should be NULL in this case.

If the arena is "growable", len specifies the original size (minimum of 1K bytes) and the grow_func parameter specifies a function that will be called when the allocator requires more memory. Note that the original buffer addr will be used only for the arena header; the first time more memory is required, the "grow" function will be called. This suggests that a minimal (1K) original buffer should be used when setting up a growable arena.

The grow function will be called with two parameters: the number of bytes required and a pointer to the arena requiring the space. The number of bytes requested will always be a multiple of M_BLKSZ (see header file). The function should return the address of a suitably large block of memory. This block does not need to be contiguous with the original arena memory. This block could be obtained from a number of sources, such as by mapping in another file (by means of mmap(2)) or by calling malloc(3) to enlarge the program's data space. If the grow function decides that it cannot provide any more space, it must return (void*)-1.

The ushdr function is currently unused and must be NULL.

adelete
Causes any resources allocated for the arena (for example, mutexes) to be freed. Nothing is done with the arena memory itself. No additional calls to any arena functions can be made after calling adelete.

amalloc
Returns a pointer to a block of at least size bytes suitably aligned for any use.

afree
Destroys the contents of a block previously allocated by amalloc, arealloc, or acalloc and makes this space available for future allocation. The argument to afree is a pointer to the block previously allocated by amalloc, arealloc, or acalloc.

Undefined results will occur if the space assigned by any of the three arena allocator functions is overrun or if some random number is handed to afree. It is always permitted to pass NULL to afree.

arealloc
Changes the size of the block pointed to by ptr to size bytes and returns a pointer to the (possibly moved) block. The contents will be unchanged, up to the lesser of the new and old sizes. In the special case of a null ptr, arealloc degenerates to amalloc. A zero size causes the passed block to be freed.

acalloc
Allocates space for an array of nelem elements of size elsize. The space is initialized to zeros.

amallocblksize
Returns the actual size of the block pointed to by ptr. The returned size may be greater than the original requested size.

amallopt
Provides for control over the allocation algorithm. The available values for cmd are defined in the header file.

The amallopt function can be called repeatedly but, for most commands, not after the first small block is allocated.

amallinfo
Provides instrumentation describing space usage. It returns the mallinfo structure defined in the header file. The structure is zero until after the first space has been allocated from the arena.

Each of the allocation routines returns a pointer to space suitably aligned for storage of any type of object.

RETURN VALUES

The acreate function returns NULL and sets errno if either len is less than 1K or the MEM_SHARED flag is passed.

The amalloc, arealloc, and acalloc functions return a NULL pointer if there is not enough available memory. When arealloc returns NULL, the block pointed to by ptr is left intact. If amallopt is called after any allocation (for most cmd arguments) or if cmd or value is invalid, nonzero is returned. Otherwise, it returns zero.

RELATED INFORMATION

Function: malloc(3)

1.8 Release Notes for Patch 591.00

This release note discusses the I/O Throttling/Smooth Sync patch.

Note

In order to activate I/O Throttling/Smooth Sync, you must also install Patch 568.00.

Note

Smooth Sync is for UNIX File System (UFS) only.

Update your `/etc/fstab` entries to enable the selected mount options on the selected UFS filesystems.

The new options are `smsync2` and `throttle`. The `smsync2` enables an alternate `smsync` policy in which dirty pages do not get flushed until they have been dirty and idle for the `smoothsync` age period (default 30 seconds). The default policy is

to flush dirty pages after being dirty for the smoothsync age period, regardless of continued modifications to the page. Note that mmaped pages always use this default policy, regardless of the smsync2 setting.

For example, change from:

```
/dev/rz12e /mnt/test ufs rw 0 2
```

to:

```
/dev/rz12e /mnt/test ufs rw,smsync2,throttle 0 2
```

Note

If you choose not to use smsync2 (which does not affect memory-mapped buffers), remove the smsync2 option from the previous string.

Append to /etc/sysconfigtab any tuning changes. See 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.

To remove this patch, follow these steps:

1. Edit the /etc/inittab and remove the following smsync lines:

   ```
   smsync:23:wait:/sbin/sysconfig -r vfs smoothsync-age=30 >
   /dev/null 2>&1
   smsyncS:Ss:wait:/sbin/sysconfig -r vfs smoothsync-age=0 >
   /dev/null 2>&1
   ```

2. Remove any additions to /etc/fstab you may have made (see the previous instructions).

Failure to remove /etc/inittab and /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. This patch introduces a smoothsync approach to writing delayed I/O requests and introduces I/O throttling.

Using smoothsync allows each dirty page to age for a specified time period before getting pushed to disk. This allows more opportunity for frequently modified pages to be found in the cache, which decreases the net I/O load. Also, as pages are enqueued to a device after having aged sufficiently, as opposed to getting flushed by the update daemon, spikes in which large numbers of dirty pages are locked on the device queue are minimized.

I/O throttling further 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:

`smoothsync-age`

You can adjust this variable from 0 (off) up to 300. This is the number of seconds a page ages before becoming eligible for being flushed to disk via the smoothsync mechanism. A value of 30 corresponds to the guarantee provided by the traditional UNIX update mechanism. Increasing this value increases the exposure of lost data should the system crash, but can decrease net I/O load (to improve performance) by allowing the dirty data to remain in cache longer. In some environments, any data that is not up to date is useless; these are prime candidates for an increased `smoothsync-age` value. The default value of `smoothsync-age` is 30.

`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 are:

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 previous 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 that 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 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.

1.9 Release Notes for Patch 534.00

The following release notes provide updated information for the `quotacheck`(8), `fsck`(8), and `fstab`(4) reference pages.

quotacheck(8) Reference Page Update

SYNOPSIS

/usr/sbin/quotacheck [-guv] filesystem ...

OLD> /usr/sbin/quotacheck -a [-guv] [-l number]
NEW> /usr/sbin/quotacheck -a [-guv] [-l number] [-t [no]type]

FLAGS

OLD> -a Checks all file systems identified in the /etc/fstab file as read/write with disk quotas.

NEW> -a Checks all UFS and AdvFS file systems identified in the /etc/fstab file as read/write with userquota and/or groupquota options specified, and a pass number of 1 or greater. If the -t option is specified, only the file systems of the specified type will be checked. Alternatively, if type is prefixed with 'no', then the valid file systems in the /etc/fstab file that do not have that type will be checked.

OLD> -l number Specifies the number of times to perform disk quota checking.

NEW> -l number Specifies the maximum number of parallel quotacheck processes to run at one time.

NEW> -t [no]type
NEW> Specifies the file system type. The supported file systems are as follows:

advfs - Advanced File System (AdvFS)

ufs - UNIX File System (UFS)

See fstab(4) for a description of file system types. If the 'no' prefix is used, all of the previous file types except the one specified are checked.

Note, the -t flag is only valid when used with the -a flag.

DESCRIPTION

OLD> The quotacheck command examines each specified file system, builds a table of current disk usage, and compares this table against that stored in the disk quota file for the file system. If any inconsistencies are detected, both the quota file and the current system copy of the incorrect quotas are updated. Each file system must be mounted with quotas enabled.

NEW> The quotacheck command examines each specified file system, builds a table of current disk usage, and compares this table against that stored in the disk quota file for the file system. If any inconsistencies are detected, both the quota file and the current system copy of the incorrect quotas are updated.

OLD> The quotacheck command runs parallel passes on file systems using the number specified in the fsck field of the file system's entry in the /etc/fstab file. The quotacheck command only checks file systems with pass number 1 or higher in the fsck field. A file system with no pass number is not checked.

NEW> The quotacheck -a command runs parallel passes on file systems using the number specified in the /etc/fstab pass number field. The quotacheck command only checks file systems with pass number 1 or higher in the fsck field. A file system with no pass number is not checked.

OLD> For both UFS file systems and AdvFS filesets, you should assign the root file system a fsck field value of 1, and a value of 2 or higher to other file systems. See fstab(4) for more information.

NEW> For both UFS file systems and AdvFS filesets, you should assign the root file system a pass number of 1, and a value of 2 or higher to other file systems. See fstab(4) for more information.

OLD> The quotacheck command checks only file systems that have the userquota or groupquota option specified in the /etc/fstab file.

NEW> The quotacheck command checks only file systems that are mounted. UFS file systems must also have userquota and/or groupquota options specified in the /etc/fstab file. The userquota and groupquota options are only needed for AdvFS file systems if quotas are actually going to be enforced or if they are to be selected with the -a option.

fsck(8) Reference Page Update

OLD> When the system boots, the fsck program is automatically run with the -p flag. The program reads the /etc/fstab file to determine which file systems to check. Only partitions that are specified in the fstab file as being mounted “rw” or “ro” and that have a nonzero pass number are checked. File systems that have a pass number 1 (usually only the root file system) are checked one at a time. When pass 1 completes, all the remaining file systems are checked, with one process running per disk drive.

NEW> When the system boots, the fsck program is automatically run with the -p flag. The program reads the /etc/fstab file to determine which file systems to check. Only partitions that are specified in the fstab file as being mounted “rw” or “ro” and that have a nonzero pass number are checked. File systems that have a pass number 1 (usually only the root file system) are checked one at a time. When pass 1 completes, the remaining pass numbers are processed with one parallel fsck process running per disk drive in the same pass.

NEW> The per disk drive logic is based on the /dev/disk/dsk0a syntax where different partition letters are treated as being on the same disk drive. Partitions layered on top of an LSM device may not follow this naming convention. In this case unique pass numbers in /etc/fstab may be used to sequence fsck checks.

fstab(4) Reference Page Update

userquota [=filename] and groupquota [=filename]

If quotas are to be enforced for users or groups, one or both of the options must be specified. If userquota is specified, user quotas are to be enforced. If groupquota is specified, group:

OLD> quotas are to be enforced.

NEW> quotas are to be enforced (see quotaon and quotaoff(8)).

OLD> For UFS file systems, the sixth field, (fsck), is used by the fsck command to determine the order in which file system checks are done at reboot time. For the root file system, specify 1 in the fsck field. For other UFS file systems, specify 2 or higher in the fsck field. Each UFS file system should have a unique fsck value.

NEW> For UFS file systems, the sixth field, (pass number), is used by the fsck and quotacheck commands to determine the order in which file system checks are done at reboot time.

For the root file system, specify 1 in the fsck field. For other UFS file systems specify 2 or higher in the pass number field.

OLD> For AdvFS filesets, the sixth field is a pass number field that allows the quotacheck command to perform all of the consistency checks needed for the fileset. For the root file system, specify 1 in the fsck field. Each AdvFS fileset in an AdvFS file domain should have a unique fsck value, which should be 2 or higher.

NEW> For AdvFS filesets, the sixth field is a pass number field that allows the quotacheck command to perform all of the consistency checks needed for the fileset. For the root file system, specify 1 in the fsck field. For other AdvFS file systems specify 2 or higher in the pass number field.

OLD> File systems that are on the same disk are checked sequentially, but file systems on different disks are checked at the same time to utilize parallelism available in the hardware. If the sixth field is not present or zero, a value of 0 is returned and the fsck command assumes that the file system does not need to be checked.

NEW> File systems that are on the same disk or domain are checked sequentially, but file systems on different disks or domains but with the same or greater than 1 pass number are checked at the same time to utilize parallelism available in the hardware. When all the file systems in a pass have completed their checks, then the file systems with the numerically next higher pass number will be processed.

NEW> The UFS per disk drive logic is based on the /dev/disk/dsk0a syntax where different partition letters are treated as being on the same disk drive. Partitions layered on top of an LSM device may not follow this naming convention. In this case unique pass numbers may be used to sequence fsck and quotacheck processing. If the sixth field is not present or 0, a value of 0 is returned and the fsck command assumes that the file system does not need to be checked.

1.10 Release Notes for Patch 581.00

If the system configurable parameter, `lsm:lsm_V_ROUND_enhanced` is set (value = 1), the enhanced read round robin policy is activated. This new policy stores the last block accessed by the previous IO request. When returning for another block in round robin (`V_ROUND`) mode, that value is compared to the current read. If it is within a predefined, user-configurable value (`lsm:lsm_V_ROUND_enhance_proximity`), then the same plex is used. Otherwise the next plex is used as for a normal round robin behavior.

The two new additional tunable parameters are `lsm_V_ROUND_enhanced` set to 1 by default (`V_ROUND` read is activated) and `lsm_V_ROUND_enhance_proximity` is set to 512 by default.

Append any tuning changes to `/etc/sysconfigtab`. Refer to the TUNING notes below for a description of the new `lsm_V_ROUND_enhanced` and `lsm_V_ROUND_enhance_proximity` tunables. These tunables are configured in the `lsm` stanza. The following three lines are an example:

```
lsm:
 lsm_V_ROUND_enhanced = 1
 lsm_V_ROUND_enhance_proximity = 1024
```

Note

If you already have an `lsm` stanza in your `sysconfigtab` file, then just add the two `lsm_V_ROUND` entries.

TUNING

The purpose of this patch is to increase performance with sequential reads. This patch introduces a new enhanced round robin mode where the last block read is now compared to the next block to read, and a check is added to see if last block number–next block number is less than or equal to `lsm_V_ROUND_enhance_proximity`. If it is, read from the same plex. This attempts to hit the disk cache, thereby increasing performance.

The relevant tunable variables are:

`lsm_V_ROUND_enhanced` This variable activates the new enhanced round robin read policy if it is set to TRUE (1). Otherwise the policy is deactivated.

DEFAULT = 1

`lsm_V_ROUND_enhance_proximity` This variable provides the proximity in which the last read and new read most lie in an attempt to read data from the disk's cache by reading from the same plex. The variable can be adjusted from 0 to 4096.

DEFAULT = 512

2

Summary of Base Operating System Patches

This chapter summarizes the base operating system patches included in Patch Kit-0004.

Table 2–1 lists patches that have been updated.

Table 2–2 provides a summary of patches.

Table 2–1: Updated Base Operating System Patches

Patch IDs	Change Summary
469.00, 470.00, 472.00, 473.00, 477.00, 479.00, 485.00, 488.00, 489.00, 491.00, 494.00, 495.00, 496.00, 503.00, 504.00, 505.00, 514.00, 516.00, 525.00, 527.00, 540.00, 541.00, 543.00, 546.00, 556.00, 562.00, 563.00, 565.00, 568.00, 571.00, 575.00, 577.00, 578.00, 599.00, 603.00	New
Patch 258.00	Superseded by Patch 468.00
Patches 6.00, 40.00, 445.00, 446.00, 447.00, 221.00, 449.00	Superseded by Patch 471.00
Patches 32.00, 250.00	Superseded by Patch 475.00
Patches 327.00, 328.00, 452.00, 454.00	Superseded by Patch 476.00
Patches 33.00, 455.00, 450.00, 451.00, 474.00	Superseded by Patch 478.00
Patches 79.00, 358.00	Superseded by Patch 506.00
Patches 300.00, 301.00	Superseded by Patch 509.00
Patches 111.00, 116.00, 308.00, 427.00, 368.00	Superseded by Patch 521.00
Patches 61.00, 86.00, 141.00, 142.00, 148.00, 158.00, 242.00, 45.00, 263.00, 95.00, 71.00, 312.00, 316.00, 366.00, 378.00, 384.00, 390.00, 400.00, 320.00, 379.00, 433.00, 408.00, 512.00	Superseded by Patch 534.00
Patches 9.00, 59.00, 78.00, 14.00, 22.00, 225.00, 232.00, 233.00, 255.00, 338.00, 344.00, 357.00, 381.00, 401.00, 498.00	Superseded by Patch 536.00
Patches 48.00, 85.00, 243.00, 82.00, 297.00, 296.00, 315.00, 323.00, 376.00, 431.00, 508.00, 524.00	Superseded by Patch 545.00
Patches 163.00. 486.00, 542.00	Superseded by Patch 547.00
Patches 157.00, 365.00, 518.00	Superseded by Patch 555.00
Patches 103.00, 151.00, 548.00	Superseded by Patch 558.00
Patches 144.00, 153.00, 265.00, 535.00, 551.00	Superseded by Patch 559.00
Patches 325.00, 382.00	Superseded by Patch 564.00
Patches 97.00, 484.00, 537.00	Superseded by Patch 566.00
Patch 394.00	Superseded by Patch 567.00
Patch 165.00	Superseded by Patch 580.00
Patches 26.00, 80.00	Superseded by Patch 581.00
Patches 118.00, 138.00, 544.00	Superseded by Patch 582.00
Patches 19.00, 550.00	Superseded by Patch 583.00

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

Patch 23.00	Superseded by Patch 585.00
Patches 15.00, 81.00, 270.00, 432.00, 557.00	Superseded by Patch 586.00
Patches 154.00, 415.00	Superseded by Patch 588.00
Patches 72.00, 492.00, 538.00	Superseded by Patch 590.00
Patches 58.00, 90.00, 93.00, 52.00, 56.00, 83.00, 87.00, 88.00, 67.00, 65.00, 100.00, 91.00, 102.00, 104.00, 108.00, 110.00, 11.00, 94.00, 96.00, 139.00, 137.00, 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, 195.00, 196.00, 197.00, 198.00, 199.00, 200.00, 201.00, 202.00, 203.00, 204.00, 205.00, 206.00, 114.00, 207.00, 259.00, 256.00, 42.00, 290.00, 293.00, 295.00, 252.00, 298.00, 310.00, 318.00, 136.00, 330.00, 339.00, 355.00, 356.00, 367.00, 370.00, 373.00, 375.00, 380.00, 385.00, 395.00, 398.00, 399.00, 405.00, 406.00, 407.00, 412.00, 417.00, 418.00, 426.00, 428.00, 161.00, 434.00, 337.00, 227.00, 283.00, 50.00, 302.00, 388.00, 413.00, 429.00, 480.00, 481.00, 482.00, 490.00, 497.00, 500.00, 507.00, 510.00, 511.00, 513.00, 515.00, 519.00, 520.00, 528.00, 529.00, 533.00, 539.00, 560.00, 570.00, 572.00, 576.00, 589.00, 266.00, 593.00, 517.00, 526.00, 552.00, 532.00, 101.00, 105.00, 143.00, 149.00, 150.00, 332.00, 334.00, 155.00, 341.00, 522.00, 549.00, 574.00, 396.00, 587.00	Superseded by Patch 591.00
Patches 99.00, 69.00, 115.00, 159.00, 164.00, 326.00, 329.00, 348.00, 386.00, 389.00, 483.00, 523.00, 553.00, 554.00, 573.00, 579.00	Superseded by Patch 594.00
Patch 251.00	Superseded by Patch 596.00
Patches 124.00, 461.00. 463.00, 595.00	Superseded by Patch 597.00
Patches 44.00, 126.00, 131.00, 132.00, 208.00, 209.00, 210.00, 211.00, 212.00, 213.00, 214.00, 215.00, 216.00, 217.00, 218.00, 219.00, 113.00, 220.00, 294.00, 353.00, 354.00, 359.00, 371.00, 397.00, 409.00, 411.00, 419.00, 422.00, 299.00, 425.00, 487.00, 493.00, 499.00, 501.00, 502.00, 530.00, 531.00, 561.00, 569.00, 584.00, 383.00, 592.00, 598.00, 600.00, 601.00	Superseded by Patch 604.00
Patches 128.00, 271.00, 459.00, 602.00	Superseded by Patch 605.00

Table 2–2: Summary of Base Operating System Patches

Patch IDs	Abstract
Patch 3.00 OSF435CDE-405007	**Patch:** CDE File Manager (dtfile) Command Correction **State:** Existing The patch fixes a problem in which the CDE file manager (dtfile) fails to open files that use dtpad as the exec'd action. This includes both double-clicking on the file and using Open from the Selected pull-down menu.
Patch 4.00 OSF435CDE-405008A	**Patch:** dtterm Escape Sequence Fixes **State:** Existing This patch fixes a problem in which the dtterm Terminal Emulator fails to send the DO and HELP user-defined Keys when depressed. It also fixes a problem in which proper escape sequences for F10, DO, and HELP were not being reported when the keys were depressed.

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

Patch 5.00 OSF435CDE-405009	**Patch:** dtcm (CDE) Calendar Manager Correction **State:** Existing This patch fixes a problem where the Common Desktop Environment (CDE) calendar manager (dtcm) will hang if you enter an appointment 25 days or more in advance when there are no intervening appointments.
Patch 7.00 OSF435DX-405009	**Patch:** dxdiff Core Dumps **State:** Existing This patch fixes a problem where dxdiff will core dump when comparing files with long lines.
Patch 8.00 OSF435-405290	**Patch:** last Command Corrections **State:** Existing This patch fixes a problem with the last(8) command. Users that have logged out of a system are still listed as active in the /var/adm/wtmp accounting file.
Patch 12.00 OSF435-405329	**Patch:** Security (SSRT0548U, SSRT0412U) **State:** Existing A potential security vulnerability has been discovered in the tip command, where under certain circumstances users may gain unauthorized access. Compaq has corrected this potential vulnerability.
Patch 16.00 OSF435-405360	**Patch:** expr Truncating Leading Zeros **State:** Existing This patch fixes a problem with the expr command in which the leading zeros are truncated if CMD_ENV is set to bsd.
Patch 18.00 OSF435-405369	**Patch:** rpc.lockd Pending Lock Requests Not Retransmitted **State:** Existing This patch fixes the following problems: • Moves locked files from the message queue to the held list once. • Adds code to allow locked files left over from a server reboot, to timeout and be transmitted to the server.
Patch 21.00 OSF435-405377	**Patch:** pty Kernel Memory Fault Panic **State:** Existing This patch fixes a panic caused by freeing a pty on a reopen of the controlling tty.
Patch 27.00 OSF435-405422	**Patch:** Fix for edquota Command **State:** Existing This patch fixes a problem with the edquota utility, which prevented a user from creating quotas for UIDs or GIDs that did not already exist in the /etc/passwd or /etc/group files.
Patch 28.00 OSF435-405447	**Patch:** Kernel Build config Command Core Dumps **State:** Existing This patch fixes a problem in which the kernel build config command (obj/alpha/kernel/bin/config) core dumps if the fopen function fails.
Patch 29.00 OSF435-405449	**Patch:** Bourne Shell Performance Improvement **State:** Existing This patch fixes a problem where the performance of the Bourne shell may be slow when there are many automounted directories in the search path (as defined by the PATH environment variable).

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

Patch 35.00 OSF435X11-405013	**Patch:** X Server May Core Dump on DMS Client System **State:** Supersedes patch OSF435X11-405012 (34.00) This patch corrects the following: • Fixes a problem where the X server may generate a core dump during shutdown on a dataless management services (DMS) client system. • Fixes a problem that prevents an X server from starting. The following error message is displayed: Fatal server error: Cannot establish any listening sockets. Make sure an X server isn't already running.
Patch 37.00 OSF435CDE-425009	**Patch:** dtksh Fails to Create Windows **State:** Existing This patch fixes a problem where dtksh (the version of the Korn shell provided with the Common Desktop Environment (CDE)) fails to create windows on the local display and gives the following error: Xlib: connection to ":0.0" refused by server Xlib: Client is not authorized to connect to Server Error: Can't open display: :0.0 This problem affects the CDE applications which use dtksh scripts such as dtlp, the file printing utility, and the calendar and mail database conversion utilities. Because dtlp is affected, printing from within many CDE applications does not work (the printer-selection window is not displayed).
Patch 38.00 OSF435DX-425012	**Patch:** Incorrect Error Msgs From svrServer_mib **State:** Supersedes patch OSF435DX-410004 (36.00) This patch corrects the following: • Corrects the following error message seen in the daemon.log file: svrSystem_mib[1434]:svrSystem_mib **ERROR esnmp_poll.c line 685: Method routine returned invalid status:2 • Corrects unnecessary warning messages from the svrServer_mib when it could not find the threasholds.dat file.
Patch 41.00 OSF435DX-425017	**Patch:** Fixes to useradd and usermod Commands **State:** Supersedes patch OSF435DX-425013 (39.00) This patch corrects the following: • Fixes a problem where adding an NIS user via useradd required that the user's primary group exist in NIS as well. The primary group does not need to be in the NIS database when adding a NIS user. • Fixes the problem where usermod -g <group> <user> will lock the user account if it is unlocked.
Patch 46.00 OSF435-425271	**Patch:** AdvFS Boot Code Problem Traversing Symbolic Links **State:** Existing This patch fixes a problem in which AdvFS boot code has trouble traversing symbolic links.
Patch 47.00 OSF435-425274	**Patch:** adduser Command Correction **State:** Existing This patch fixes a problem in which the adduser(8) command puts user directories in /usr instead of /usr/users.

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

Patch 49.00 OSF435-425283	**Patch:** Environ. Monitoring Fails to Start on Bootup **State:** Existing This patch fixes a problem where Environmental Monitoring sometimes fails to start on boot up. The following error message is written to the log file: Either svrSystem_mib is not running or envmon.mod module is not loaded.
Patch 51.00 OSF435-425295	**Patch:** find Command Correction **State:** Existing This patch fixes the find command in which files in directories which were mounted with the -fstype nfsv2 argument were not found.
Patch 53.00 OSF435-425303	**Patch:** rmfdmn Displays Messages on Standard Error Device **State:** Existing This patch fixes a problem with the rmfdmn command, which previously displayed success messages on the standard error device instead of the standard output device.
Patch 54.00 OSF435-425314	**Patch:** faa FDDI Driver Causes Kernel Memory Fault **State:** Existing This patch fixes a kernel memory fault problem that occurs with the faa FDDI driver.
Patch 60.00 OSF435-425348	**Patch:** Memory Errors Logged to System Console **State:** Existing This patch fixes a problem in which correctable memory errors are being logged to the system console as well as to the binary error log.
Patch 62.00 OSF435-425354	**Patch:** showfile Command Incorrectly Returns Error Status **State:** Existing This patch fixes a problem with the showfile command, which incorrectly returned an error status when it attempted to display a file that was a symbolic link.
Patch 63.00 OSF435-425355	**Patch:** Invalid Error Msgs on AlphaServer 4100 **State:** Existing This patch fixes a situation on the AlphaServer 4100 where a system heavily loaded with I/O traffic will exhibit error messages from the environmental monitoring subsystem which are not, in fact, errors.
Patch 64.00 OSF435-425356	**Patch:** savecore Incorrectly Reports Dumped Bytes **State:** Existing This patch fixes a problem in which savecore incorrectly reports a negative number of dumped bytes. This problem may be seen when doing a full crash dump on a system that has more then 2 GB of memory.
Patch 66.00 OSF435-425361	**Patch:** crontab Incorrectly Deleting Files **State:** Existing This patch prevents the crontab file from incorrectly deleting files found in file systems mounted under the /var/preserve, /tmp, and /var/tmp directories.

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

Patch 74.00 OSF435-425403	**Patch:** select System Call May Cause System Hang **State:** Supersedes patch OSF435-425392 (73.00) This patch corrects the following: • A call to the select() system call may hang or incorrectly indicate that there is a message waiting from a terminal when there is nothing there. • Fixes a problem in which the system may panic with the following error message "kernel memory fault".
Patch 76.00 OSF435-425412	**Patch:** df (vdf) Support for AdvFS Filesets and Domains **State:** Existing The vdf program is introduced to DIGITAL UNIX V4.0D as a variation of the df program that is especially suited to use with AdvFS domains and filesets.
Patch 89.00 OSF435-012	**Patch:** Machine Server Sys Calls Not Type Checking Args **State:** Existing This patch fixes a problem where the machine server system calls are not being type checked properly, potentially causing system crashes by unprivileged programs.
Patch 92.00 OSF435-016	**Patch:** kloadsrv Halts When System is in Single User Mode **State:** Existing This patch ensures that kloadsrv remains running when the system is shut down to the single user run level.
Patch 98.00 OSF435-027	**Patch:** Compiler Problem Causes CPU EXCEPTION Errors **State:** Existing This patch fixes a compiler problem that was causing CPU EXCEPTION errors to be generated in the system binary error log. The problem was experienced during bootstrap on 2100A CPUs.
Patch 112.00 OSF435-056	**Patch:** Support for Compaq Analyze Utility **State:** Existing A new version of the binary error log daemon (/usr/sbin/binlogd) converts the internal format of each error log entry to a new format that is common across the three major Alpha operating systems: DIGITAL UNIX, OpenVMS, and Windows NT. This common format is utilized by Compaq Analyze, a new analysis utility that replaces DECevent.
Patch 120.00 OSF435CDE-405008B	**Patch:** dtterm Terminal Emulator Correction **State:** Existing This patch fixes a problem in which the dtterm Terminal Emulator fails to send the DO and HELP User Defined Keys when depressed. It also fixes a problem in which proper escape sequences for F10, DO, and HELP were not being reported when the keys were depressed.
Patch 121.00 OSF435-405328B	**Patch:** acctcom and acctcms Corrections **State:** Existing This patch corrects a small accounting problem where the measured time for a process was an integral rather than mean value.
Patch 125.00 OSF435X11-405011C	**Patch:** Security (SSRT0547U) **State:** Existing A potential security vulnerability has been discovered where, under certain circumstances, users may gain unauthorized access. Compaq has corrected this potential vulnerability.

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

Patch 140.00 OSF435-425489	**Patch:** Security Patch (SSRT0589U) **State:** Existing 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 146.00 OSF435-107	**Patch:** Fix For ATM Driver System Panic **State:** Existing This patch corrects a problem in the ATM driver which could result in data inconsistency and system panic.
Patch 147.00 OSF435-109	**Patch:** Fix For hiprof & pixie Profiling Tools **State:** Existing This patch fixes three problems in which programs instrumented with the hiprof(5) or pixie(5) profiling tool may malfunction during execution or generate inaccurate profiles.
Patch 156.00 OSF435-147	**Patch:** Fix for DECEV56_PBP DMCC Platform Code **State:** Existing This patch fixes a problem in which the platform support code for the "DECEV56_PBP" DMCC platforms is incorrectly checking if scatter gather is needed in the dma_map_load() routine.
Patch 168.00 OSF435-086	**Patch:** Fix For Problem with XTI over TCP/IP **State:** Supersedes patch OSF435-007 (119.00) This patch corrects the following: • Fixes a problem in which the xti_discon_ind() function allocates a data buffer for zero-length data. • Fixes a problem with XTI over TCP/IP when tcp_sendspace and tcp_recvspace have been decreased to 1 K. When sending 4 K data (using t_snd), the call is successful but no data has been sent and no message is returned.
Patch 169.00 OSF435-090	**Patch:** Fix for ATM CLIP Interface Memory Problem **State:** Existing This patch fixes a problem in which systems that use the Compaq Tru64 UNIX ATM CLIP interface may run out of memory.
Patch 171.00 OSF435-096	**Patch:** Fixes An EISA Device Installation Problem **State:** Existing This patch fixes a problem where the comm, floppy, and parallel port entries do not exist for the DEC5031 platform in the eisa_option_data.c file but are specified in the /etc/sysconfigtab file. This makes an installation from an EISA device impossible.
Patch 172.00 OSF435-098	**Patch:** Fix For pnvram_read Panic **State:** Existing This patch fixes a panic while prestoserve is enabled. The following error message is displayed: pnvram_read: Timed out attempting to acquire DMA semaphore
Patch 174.00 OSF435CDE-405021	**Patch:** Security (SSRT0585U) **State:** Supersedes patch OSF435CDE-405015 (173.00) 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 222.00 OSF435DX-405011	**Patch:** Fix For dxpause Program **State:** Existing This patcc fixes the problem where the dxcalendar reminder displays through the pause screen (dxpause) and remains on the top of the pause window.
Patch 223.00 OSF435-405496	**Patch:** quotaon Command Returns Incorrect Error Status **State:** Existing This patch fixes a problem in which the quotaon command returned an incorrect error status if the file system did not exist.
Patch 224.00 OSF435-405475	**Patch:** vi Editor Corrections **State:** Supersedes patches OSF435-425316 (55.00), OSF435-405510 (229.00) This patch corrects the following: • Fixes a problem with the vi editor environment variable EXINIT that occurs when EXINIT includes the editor's so subcommand. • Fixes a problem where vi puts the server port into PASSALL MODE (where XON/XOFF is no longer effective). This creates garbage in the file. • Corrects the following two problems which can occur when using vi to edit files 100 MB or larger: – The terminal settings can be disrupted causing the window to be unusable. – A core dump may occur.
Patch 228.00 OSF435-405504	**Patch:** file Cmd Interprets /etc/magic File Incorrectly **State:** Existing This patch corrects the behavior of the file command when a WAV audio file is specified as input.
Patch 230.00 OSF435-405516	**Patch:** Fix for binmail Command **State:** Existing 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 231.00 OSF435-405518	**Patch:** Fix for tail -n -r Command **State:** Existing This patch corrects erroneous behavior when the tail command is used with both the -n and -r flags.
Patch 234.00 OSF435-405540	**Patch:** Fix for yacc Parser **State:** Existing This patch fixes a problem in yacc that causes it to generate parse tables that result in the parser not executing a user-specified error recovery action.
Patch 237.00 OSF435-405552	**Patch:** Security (SSRT0556U) **State:** Existing A potential security vulnerability has been discovered where, under certain circumstances users may gain unauthorized access. Compaq has corrected this potential vulnerability.
Patch 238.00 OSF435-405553	**Patch:** Fix for mkdir -p Command **State:** Existing This patch fixes a problem with the mkdir -p command. mkdir -p would not return an error if the last component in the pathname already exists.

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

Patch 239.00 OSF435-405557	**Patch:** Fix for awk Printing Problems **State:** Supersedes patch OSF435-405482 (226.00) This patch corrects the following: • Fixes a problem in the awk command. The maximum number of fields per record was changed from 99 to 199. • Fixes problem with awk printing incorrectly.
Patch 240.00 OSF435-405559	**Patch:** LSM Cmd volrootmir -a Fails **State:** Existing This patch fixes a problem where the LSM command volrootmir -a fails if the source and target disks are not the same type.
Patch 241.00 OSF435-405561	**Patch:** Fix for POP Mail Handler **State:** Existing This patch corrects two problems with the POP mail handler: • Netscape Mail clients are unable to access their mailboxes after an initial session. The /usr/spool/pop/username.lock file is left over and must be removed manually. • The POP mail handler fails to properly rename its temp file after receiving a quit command.
Patch 244.00 OSF435-405566	**Patch:** volrecover Does Not Return Failed Status Code **State:** Existing This patch corrects a problem in which a failure of the volrecover utility will not return a failed status code.
Patch 246.00 OSF435-405569	**Patch:** Security (SSRT0546U, SSRT0542U) **State:** Supersedes patches OSF435-001C (130.00), OSF435-405568 (245.00) This patch corrects the following: • 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. • Fixes a problem in which a BIND server may find that named will place a warning message in the daemon.log that was not previously seen. • Fixes a problem in which a BIND server writes files to the /etc/namedb directory instead of the /var/tmp directory.
Patch 247.00 OSF435-405580	**Patch:** automount Daemon Hangs **State:** Supersedes patch OSF435-405374 (20.00) This patch corrects the following: • Fixes an automount problem. An automount map file entry that included a comment was being parsed incorrectly, resulting in an error. • Fixes a problem in which the automount daemon hangs when invoked by the rsh command.
Patch 248.00 OSF435X11-405014	**Patch:** Enhancement for makedepend Utility **State:** Existing This patch increases the maximum number of files that one file can depend on in the makedepend utility from 1024 to 4096.
Patch 249.00 OSF435X11-405015	**Patch:** xfs Fails When It Receives An Invalid Request **State:** Existing This patch fixes a problem where the X font server (xfs) sometimes failed with a segmentation fault when it received an invalid request.

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

Patch 253.00 OSF435-410223	**Patch:** Fix For rsh Command **State:** Existing This patch fixes a problem when using rsh to run shutdown on a client server. The correct console messages are displayed, but the system hangs instead of shutting down.
Patch 254.00 OSF435-410225	**Patch:** voldiskadm Not Working Correctly **State:** Existing This patch corrects an LSM problem where voldiskadm was not properly handling the removal and replacement of disks that were in an error state.
Patch 257.00 OSF435CDE-425011	**Patch:** Security (SSRT0571U) **State:** Supersedes patches OSF435CDE-405011 (2.00), OSF435CDE-405022 (175.00) This patch corrects the following: • Fixes a problem where dtmail can core dump when there exists long lines in Sun Mail Tool attachments. This causes a buffer overflow. • Fixes a problem where the CDE mail interface (dtmail) does not display the date and time of mail messages in the Message Header list when the time zone is set to certain time zones such as GB-Eire. • A potential security vulnerability has been discovered where, under certain circumstances, users may gain unauthorized access. Compaq has corrected this potential vulnerability.
Patch 260.00 OSF435-425443	**Patch:** Fix for doconfig -a and -m Options **State:** Supersedes patch OSF435-425445 (84.00) This patch corrects the following: • Fixes the doconfig command. The -a and -m options prompt the user if doconfig encounters a failure. The -a and -m options are supposed to be noninteractive in an situation. • The doconfig program incorrectly exits with a zero return code if a failure occurs.
Patch 261.00 OSF435-425449	**Patch:** Fix for lmf Data Problems **State:** Existing This patch fixes three /usr/sbin/lmf date problems: • lmf improperly handles two-digit dates between 2000 and 2068. • When lmf is given two consequtive commands and the first command contains a leap year date, then the date for the second command is automatically assumed to be in a leap year. • lmf did not recognize the date 29-FEB-2000.
Patch 264.00 OSF435-425468	**Patch:** tcpslice Problems Filtering tcdump Dump Files **State:** Existing This patch fixes a problem in which the tcpslice command has problems filtering tcpdump dump files when a year greater than 1999 is used as an end date.
Patch 267.00 OSF435-425495	**Patch:** rmt -s Command Returns Incorrect Status **State:** Existing This patch fixes a problem in which the rmt -s command returns an incorrect status.

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

Patch 268.00 OSF435-425510	**Patch:** Fix for scu Utility **State:** Existing This patch fixes two problems in the scu utility. The scu seek command seeks only to lba 0. scu does not correctly save mode pages.
Patch 269.00 OSF435-425512	**Patch:** restore Utility Causes Segmentation Faults **State:** Supersedes patch OSF435-425333 (57.00) This patch corrects the following: • Backups made by the dump program on pre-V4.0D systems were not being correctly restored by the V4.0D restore program. Specifically, ownership was being set to root:system in all cases. • Fixes two restore utility problems that were causing segmentation faults. Additionally, the restore utility now uses /var/tmp for temporary files: previously, it had incorrectly used /tmp.
Patch 272.00 OSF435-425525A	**Patch:** setacl Shared Library Correction **State:** Supersedes patch OSF435-405407A (24.00) This patch corrects the following: • Corrects the problem with setacl not being able to handle a user ID beginning with a numeral. • Fixes a memory leak in retrieve_file_acl.
Patch 273.00 OSF435-425525B	**Patch:** libpacl Static Library Correction **State:** Supersedes patch OSF435-405407B (122.00) This patch corrects the following: • Corrects the problem with setacl not being able to handle a user ID beginning with a numeral. • Fixes a memory leak in retrieve_file_acl.
Patch 274.00 OSF435-425533	**Patch:** kmem-debug Causes System Panic **State:** Existing This patch fixes a problem that caused a panic to occur when the generic subsystem attribute kmem-debug is set to 1 and the bparm subsystem is queried with the sysconfig -q command.
Patch 276.00 OSF435-425545	**Patch:** Fix For Rewind Cmd On TZ89 Tape Drive **State:** Existing This patch fixes a problem when using rewind command on the TZ89 tape drive. The tape subsystem returns an I/O error. It also adds support for some new devices.
Patch 277.00 OSF435-425553A	**Patch:** Fixes Problem Recognizing terminfo Settings **State:** Supersedes patch OSF435-405453A (31.00) This patch corrects the following: • Fixes a problem with the curses library. The infocmp command dumped core because two curses terminal capability tables were out of sync with each other. • Fixes problem recognizing terminfo settings for KEY_BTAB.
Patch 278.00 OSF435-425553B	**Patch:** Curses Static Library Fix **State:** Supersedes patch OSF435-405453B (123.00) This patch corrects the following: • Fixes a problem with the curses library. The infocmp command dumped core because two curses terminal capability tables were out of sync with each other. • Fixes problem recognizing terminfo settings for KEY_BTAB.

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

Patch 279.00 OSF435-425554	**Patch:** Fix for ipcs Command **State:** Existing This patch corrects a problem that prevents a user from using the ipcs command on a system whose kernel has been booted from a file that is not /vmunix.
Patch 280.00 OSF435-425570	**Patch:** Fix for spo_misc_errors errlog Errors **State:** Existing This patch fixes the cause of the spurious spo_misc_errors errlog entry on 4100 class systems.
Patch 284.00 OSF435-425600	**Patch:** Memory Corruption Problem Caused By devz **State:** Existing This patch fixes a possible memory corruption caused by devz.
Patch 285.00 OSF435-101	**Patch:** Corrupt rc.config File Problem **State:** Existing This patch fixes a problem with the corruption of the /etc/rc.config file when more than one rcmgr process attempts to write to the rc.config file.
Patch 288.00 OSF435-425571A	**Patch:** libtli/libxti Shared Library Correction **State:** Supersedes patches OSF435-425407A (75.00), OSF435-405522A (286.00) This patch corrects the following: • Fixes libtli/libxti to correctly handle a continuation data message still on the stream head. • Fixes a streams problem in libxti. The t_getprotaddr() function will cause a memory core dump if either of its second or third argument is NULL. • Fixes a problem in which an application using the X/Open Transport Interface (XTI) and the DECnet/OSI transport provider is unable to disconnect a rejected request.
Patch 289.00 OSF435-425571B	**Patch:** libtli/libxti Static Library Correction **State:** Supersedes patches OSF435-425407B (127.00), OSF435-405522B (287.00) This patch corrects the following: • Fixes libtli/libxti to correctly handle a continuation data message still on the stream head. • Fixes a streams problem in libxti. The t_getprotaddr() function will cause a memory core dump if either of its second or third argument is NULL. • Fixes a problem in which an application using the X/Open Transport Interface (XTI) and the DECnet/OSI transport provider is unable to disconnect a rejected request.
Patch 291.00 OSF435-125A	**Patch:** Security (SSRT0577U) **State:** Supersedes patch OSF435-008 (167.00) This patch corrects the following: • 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. • Adds profiling tools support for Alpha EV67 systems.

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

Patch 303.00 OSF435-077B	**Patch:** AdvFS Not Ensuring Links to /etc/fdmns Directory **State:** Supersedes patches OSF435-405320 (10.00), OSF435-405408 (25.00) This patch corrects the following: • Fixes a problem with an unclear AdvFS message. When trying to mount an AdvFS fileset on a system that did not have AdvFS installed, the following message was displayed: No such device Now, in similar cases, the following AdvFS message is displayed: Cannot mount AdvFS fileset, AdvFS not installed • Fixes a problem with AdvFS and links in the /etc/fdmns directory. Previously, AdvFS did not ensure that every link in a directory entry pointed to a block device. Now, it does. • Fixes a problem with the mount command where it sometimes kills other processes.
Patch 304.00 OSF435-188A	**Patch:** Y2K Fix for the nroff Text Formatter **State:** Existing This patch fixes a Y2K problem with the nroff text formatter in which the years after 1999 are translated to be 19xxx with 'xxx' being the number of years that have passed since 1900. So, the year 2010 is displayed as 19110.
Patch 307.00 OSF435-142	**Patch:** New Atom Driver in Developers Toolkit Update Kit **State:** Supersedes patch OSF435-078 (166.00) This patch corrects the following: • Fixes a potential binary compatibility problem with user-written Atom tools. • Provides the support needed for the Developer's Toolkit Update Kit.

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

Patch 321.00 OSF435-425582B	**Patch:** Network, Security (SSRT0546U, SSRT0542U) **State:** Supersedes patches OSF435-425407C (134.00), OSF435-001B (129.00), OSF435-024B (133.00), OSF435-129B (313.00), OSF435-130B (317.00) This patch corrects the following: • Fixes to libtli/libxti to correctly handle a continuation data message still on the stream head. • 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. • Fixes the following problems: – Hangs or unexpected termination of threaded processes with TotalView debugger. – gcc compiler reports errors when including the <pthread.h> header file. – A bug related to call system FORTRAN statement. • Introduces changes to the DECthreads libraries intended to improve the performance of threaded applications running on DIGITAL UNIX 4.0E. This patch specifically addresses the areas of thread scheduling, synchronization object performance and SMP scalability. • Fixes a problem that may cause the malloc suite of functions to show heavy mutex lock contention in multithreaded applications running on multiCPU systems. • Fixes problems in the DECthreads library for DIGITAL UNIX. Included in this patch are changes to support Ladebug enhancements and a bug fix for applications that employ SCS threads of different priorities.
Patch 324.00 OSF435-188B	**Patch:** nroff Incorrectly Translates Years After 1999 **State:** Existing This patch fixes a Y2K problem with the nroff text formatter in which the years after 1999 are translated to be 19xxx with 'xxx' being the number of years that have passed since 1900. Thusly, the year 2010 displays as 19110.
Patch 331.00 OSF435-164	**Patch:** Security (SSRT0596U) **State:** Existing 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 333.00 OSF435-166	**Patch:** System panic during dynamic config of device drivers **State:** Existing This patch fixes a system panic during dynamic configuration of device drivers. If more than one adapter for that device driver exists in the system and if one of those adapters fails the configuration, the device driver gets unloaded. The adapter still uses the device driver code, causing the system to panic with an invalid instruction fetch.

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

Patch 335.00 OSF435-168	**Patch:** Fixes several problems in the ATM subsystem **State:** Supersedes patches OSF435-091 (170.00), OSF435-425452 (262.00), OSF435-076 (305.00), OSF435-082 (306.00) This patch corrects the following: • Adds required functional support for the FORE ATM device driver, lfa. • Fixes an ATM LANE problem where the arp table grows significantly. • Fixes a problem in which systems that use the DIGITAL UNIX ATM LANE interface may panic with the following message. kernel memory fault • Corrects a kernel memory fault, an illegal instruction fault and an ILMI cold start trap from the ATM subsystem. • Fixes the following problems in the ATM subsystem: – Creation of multiple ATM ELANs. – Duplicate PPA registrations to the CMM. – ATM ELAN fails to come up after the APEX switch is rebooted.
Patch 336.00 OSF435-169	**Patch:** Network, Security (SSRT0559U) **State:** Supersedes patch OSF435-005 (109.00) This patch corrects the following problems: • 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. • Fixes a problem in which a system can hang when inetd tries to start a daemon listed in inetd.conf that is not installed on the system. This can occur when a user attempts to telnet to the port reserved for the nonexistent daemon.
Patch 340.00 OSF435-173	**Patch:** Fix for simple_lock system panic **State:** Existing This patch fixes a system panic with the following panic string: simple_lock: time limit exceeded
Patch 342.00 OSF435-175	**Patch:** Fix for SCSI and tape subsystems **State:** Existing This patch fixes a problem within the SCSI and tape subsystems, where an expression was not being evaluated properly.
Patch 343.00 OSF435-176	**Patch:** Fix for ace eisa driver problem **State:** Supersedes patch OSF435-106 (145.00) This patch corrects the following: • Fixes the following two problems: – When using tip or any other method over the serial com lines to a receiver that sends frequent xoff/xon, characters are randomly repeated. – On a DECstation 2000/300, the second com port (tty01) does not get configured. An error message "ksh: /dev/tty01: cannot create" is displayed when the tty01 port is accessed. • Fixes a problem with the ace EISA driver. If an ace driver is configured in the kernel but not found at device probe time, a call to the open routine will crash the O/S with a kernel memory fault.

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

Patch 345.00 OSF435-178	**Patch:** Fix for DE20x driver **State:** Existing This patch fixes a problem in the DE20x driver. On a system with a DE20x driver installed, the system panics with a kernel memory fault the moment the interface is connected to the repeater.
Patch 346.00 OSF435-179	**Patch:** Fix for rsh hang **State:** Existing This patch fixes rsh(1) hanging forever in select().
Patch 347.00 OSF435-180	**Patch:** Increases external limit symbol handled by ar cmd **State:** Existing This patch eliminates the previous limitation on the maximum number of external symbols that could be handled by the ar command.
Patch 351.00 OSF435-187	**Patch:** Allows syslog forwarding from any host **State:** Supersedes patch OSF435-425369 (68.00) This patch corrects the following: • Fixes a problem in which syslogd will core dump if /etc/syslog.auth file has greater than 23 lines. • Allows syslog forwarding from any host if the /etc/syslog.auth file is not present.
Patch 352.00 OSF435-189	**Patch:** LSM ignores privlen and nconfig parameters **State:** Existing This patch fixes a problem in LSM. The privlen and nconfig parameters were being ignored by LSM no matter what they were set to.
Patch 360.00 OSF435-198	**Patch:** Fixes a problem with pyxis systems **State:** Existing This patch fixes a problem with pyxis systems. These systems generate extra interrupts when PCI interrupts are processed.
Patch 361.00 OSF435-199	**Patch:** Adds DC21143-xD Errata V4.0 support for tulip **State:** Supersedes patch OSF435-131 (152.00) This patch corrects the following: • Fixes a problem with a DE504-BA device in an AS800 system with a second SCSI controller on the shared PCI bus. Incoming datagrams and messages are lost when the device resets and stops working for approximately two seconds. • Fixes a problem in the tulip driver. The tulip driver needs to support DC21143-xD Errata V4.0 for ethernet connections. This chip is currently being used on Compaq Professional Workstation XP1000 (as well as several others in the near future).
Patch 362.00 OSF435-200	**Patch:** Fix for DLPI problem **State:** Existing This patch fixes a problem with DLPI. It is not possible to configure DLPI's maximum link parameters. Therefore max_links and max_macs parameters have been made configurable using sysconfig.
Patch 363.00 OSF435-201	**Patch:** Fix for NFS problems **State:** Existing This patch corrects the following: • When starting or stopping NFS, NFS was not checking for NFS daemons running. • rpc.pcnfsd was causing core dumps when receiving a SIGTERM signal.

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

Patch 364.00 OSF435-203	**Patch:** Incorrect file dates restored when using pax **State:** Supersedes patches OSF435-425414 (77.00), OSF435-425573 (281.00) This patch corrects the following: • Fixes a problem in which the pax program (invoked as pax, tar, or cpio) incorrectly handles files larger than 4 GB in size. • 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. • Fixes a problem that caused incorrect file dates to be restored when pax was used to copy files. The problem occurred in the following cases: – If the file was a nonempty directory – If the file was the target of another symbolic link
Patch 369.00 OSF435-208	**Patch:** Fix for disklabel -R option **State:** Existing This patch enables the disklabel -R option to accept the invented_geometry flag as valid input in a replacement label.
Patch 372.00 OSF435-211	**Patch:** DECnet/OSI unresolved symbol:scc_configure error **State:** New This patch fixes a problem in which systems that use the Compaq Tru64 UNIX and install DECnet/OSI and WDD would get the following error message when attempting to build a kernel: unresolved symbol:scc_configure
Patch 374.00 OSF435-214	**Patch:** Fixes I/O hang in ATA driver **State:** Supersedes patch OSF435-063 (117.00) This patch corrects the following: • Enable ATAPI Iomega ZIP drives to do I/Os of a multiple of 64 KB. This is required to be able to support the ATAPI Iomega ZIP drive. • Fixes occasional I/O hangs in the ATA driver.
Patch 377.00 OSF435-220	**Patch:** stdhosts cannot handle lines longer than 256 chars **State:** Existing 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: stdhost:malformed line "ignored"
Patch 387.00 OSF435-230	**Patch:** dbx Command Corrections **State:** Supersedes patches OSF435-425383 (70.00), OSF435-425254 (43.00), OSF435-425536 (275.00) This patch corrects the following: • Fixes a problem with dbx when debugging programs that have large source files. In some cases dbx may abort with a segmentation fault. • Fixes a dbx problem with listing a large FORTRAN program that contains alternate entry points. • This patch is required for users who wish to view user stacktraces from full crash dumps with dbx. • Fixes a problem in viewing a variable subrange parameter from a Pascal module while using dbx.

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

Patch 391.00 OSF435-236	**Patch:** Pressing keys during firmware transition causes crash **State:** Existing This patch fixes a problem in which the system was consistently crashing by pressing keys during the transition from firmware callback to OS console handling.
Patch 393.00 OSF435-238	**Patch:** Fixes problem in DMA **State:** New This patch fixes a problem in DMA. Possible data loss on writes or stale data on reads could occur.
Patch 402.00 OSF435-248	**Patch:** Fix for kdbx **State:** Supersedes patch OSF435-232B (456.00) This patch corrects the following: • Fixes a problem with kdbx. A core file created by kdbx was left in the root directory when recovering from a system crash. • Fixes a problem with kdbx. The trace command was showing all threads of a process when using the option that should show only selected threads.
Patch 403.00 OSF435-249	**Patch:** Fix for invalid malloc message in mfs **State:** Supersedes patch OSF435-184 (350.00) This patch corrects the following: • Fixes a problem with the newfs command. When the newfs -N command was run on a mounted file system, it returned an error message similar to the following: newfs: /dev/rrz0c: is marked in the disklabel as in use by: 4.2BSD • Fixes invalid malloc message in mfs.
Patch 404.00 OSF435-250	**Patch:** MC1 or 1.5 will not configure with EV6 8x00 **State:** Supersedes patch OSF435-044 (106.00) This patch corrects the following: • Adds support for the Memory Channel 2 controller in TCR environment. • Fixes a problem where an MC1 or MC1.5 will not configure with an EV6 8x00.
Patch 414.00 OSF435-263	**Patch:** System hang in audit code prevents rlogins **State:** Supersedes patch OSF435-405451 (30.00) This patch corrects the following: • Fixes a problem in which audit records are generated for selected operations against objects that are not in the filesystem. • Fixes a problem where systems could hang in the audit code preventing rlogins or telnets into it.
Patch 416.00 OSF435-265A	**Patch:** Fixes a class_admin/class_daemon problem **State:** Existing This patch fixes a class_admin/class_daemon problem. When a PID had been added to a class it can not be removed from the class scheduler until the process terminates or the class_scheduler has been stopped.
Patch 420.00 OSF435-269	**Patch:** Fix for system panic in dqget **State:** Existimg This patch fixes a problem where the system can panic with a "kernel memory fault" in dqget.

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

Patch 421.00 OSF435-270	**Patch:** Fix for su command core dump problem **State:** Existing This patch fixes a problem in which the su command core dumps when calling an application using setenv and putenv.
Patch 423.00 OSF435-272	**Patch:** crashdc utility does not check for presence of kdbx **State:** Existing This patch fixes a problem in which crashdc was not checking for the presence of kdbx.
Patch 424.00 OSF435-273	**Patch:** Fix for sysconfig -q kio error **State:** Supersedes patch OSF435-425591 (282.00) This patch corrects the following: • Fixes a panic seen when accessing the kio subsystem (such as with consvar) with improper arguments. The panic was caused by a kernel double-free, and would most likely be seen as a corruption in either the 64- or 96-byte bucket (buckets 2 and 16). • Fixes a problem where the sysconfig -q kio command will return the following subsystem error: function not implemented
Patch 430.00 OSF435-279A	**Patch:** Fix for libots3 run-time library **State:** New This patch corrects the failure to check the return status after certain system calls caused a problem in the libots3 run-time library. The libots3 run-time library supports OpenMP parallel applications.
Patch 435.00 OSF435-285	**Patch:** Security (SSRT0583U, SSRT0583Z) **State:** Supersedes patch OSF435-405548 (236.00) 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 437.00 OSF435-337	**Patch:** Fixes panic for AlphaServer GS140/GS60 configurations **State:** Supersedes patches OSF435-159 (160.00), OSF435-162 (162.00) This patch corrects the following: • Adds AlphaServer 8200/8400 error log support for Alpha EV67 systems. • Resolves corrupt EV6 binary error log entries for IOP detected UDE (Uncorrectable Data Error) packets on AlphaServer 8200/8400 platforms. • Fixes a problem on some AlphaServer GS140/GS60 configurations where a simple lock timeout or TB shoot ack timeout panic may occur.
Patch 439.00 OSF435CDE-011	**Patch:** Support for Euro-currency symbol using UTF-8 locales **State:** Existing This patch provides support in the Common Desktop Environment for the Euro currency symbol using the UTF-8 Unicode locales.

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

Patch 440.00 OSF435CDE-012	**Patch:** Security (SSRT0614U) **State:** Supersedes patch OSF435CDE-405010 (1.00) This patch corrects the following: • Fixes the following problems with the CDE Calendar Manager: – The calendar manager service daemon (rpc.cmsd) core dumps when processing a calendar database file containing invalid entries. – Repeating appointments with a frequency of daily are sometimes displayed incorrectly by the calendar manager (dtcm). – The calendar manager (dtcm) will complain that it cannot connect to the calendar manager service daemon (rpc.cmsd) and rpc.cmsd will repeatedly start and die with constantly changing PIDs. • 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 442.00 OSF435CDE-007	**Patch:** dtfile does not work correctly in restricted mode **State:** Supersedes patch OSF435CDE-405023 (176.00) This patch corrects the following: • Fixes a problem where the CDE File Manager (dtfile) sometimes left defunct processes. • Fixes a problem where the Common Desktop Environment (CDE) File Manager (dtfile) did not work correctly in restricted mode.
Patch 443.00 OSF435CDE-008	**Patch:** Security (SSRT0600U) **State:** Supersedes patches OSF435CDE-010 (438.00), OSF435CDE-006 (441.00) This patch corrects the following: • Fixes a problem with the CDE desktop login screen in which logins for users with 8-character login names are rejected. • 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. • Fixes a problem where dtlogin may incorrectly set the permissions of /var to 775. It also fixes a problem where dtlogin may incorrectly set the umask to 002 for csh users.
Patch 444.00 OSF435CDE-009A	**Patch:** dxaccounts gets a BadPixmap error **State:** Existing 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 448.00 OSF435DX-008	**Patch:** diskconfig fails when creating AdvFS partition **State:** Existing This patch fixes a problem where, when creating an AdvFS partition, the disk configuration utility (/usr/sbin/diskconfig) failed with the following error: Error in Tcl Script Error: can't read "dskdir": no such variable

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

Patch 453.00 OSF435X11-007	**Patch:** X server crashes when viewing tiff images **State:** Existing This patch fixes a problem where viewing certain tiff images with an image viewer crashed the X server.
Patch 457.00 OSF435-265B	**Patch:** libclass static library fix **State:** Existing This patch fixes a class_admin/class_daemon problem. When a PID had been added to a class it cannot be removed from the class scheduler until the process terminates or the class_scheduler has been stopped.
Patch 458.00 OSF435-279B	**Patch:** Static library fix for libots3 **State:** Existing This patch corrects the failure to check the return status after certain system calls caused a problem in the libots3 run-time library. The libots3 run-time library supports OpenMP parallel applications.
Patch 460.00 OSF435X11-009B	**Patch:** X11 support for Euro currency with UTF-8 locales **State:** Existing This patch provides suppport in the X11 Environment for the Euro currency symbol using the UTF-8 Unicode locales.
Patch 462.00 OSF435CDE-009B	**Patch:** Static library fix for dxaccounts **State:** Existing 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 464.00 OSF435-405470	**Patch:** Security (SSRT0583U, SSRT0590U, SSRT0567U) **State:** Supersedes patches OSF435-405337 (13.00), OSF435-405547 (235.00), OSF435-183 (349.00), OSF435-237 (392.00) This patch corrects the following: • Corrects several problems with the at, cron, and crontab commands. • 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. • Fixes a problem with crontab in which, when root runs =crontab -e user, the user's crontab file is edited and saved, but it is not re-read by the cron daemon. Instead root's crontab file is re-read.
Patch 465.00 OSF435CDE-405013	**Patch:** Security (SSRT0566U) **State:** Existing A potential security vulnerability has been discovered where, under certain circumstances, users may gain unauthorized access. Compaq has corrected this potential vulnerability.
Patch 466.00 OSF435-207B	**Patch:** Fix for C++ V6.2 compiler **State:** Existing This patch fixes the name demangling for the tools that print symbol table names generated by the C++ V6.2 compiler. This problem will only occur for most C++ objects compiled with the ANSI options.

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

Patch 467.00 OSF435-207C	**Patch:** Fix for C++ objects compiled with ANSI options **State:** Supersedes patches OSF435-125B (292.00), OSF435-141B (309.00), OSF435-258 (410.00) This patch corrects the following: • Adds profiling tools support for Alpha EV67 systems. • Provides the support needed by the Developers' Toolkit Update Kit. These updates will not install unless this patch is installed. • Fixes a problem where prof -pixie -asm would dump core if the executable being profiled contains extremely long symbol names. • Fixes the name demangling for the tools that print symbol table names generated by the C++ V6.2 compiler. This problem will only occur for most C++ objects compiled with the ANSI options.
Patch 468.00 OSF435CDE-013	**Patch:** Security (SSRT0615U) **State:** Supersedes patch OSF435CDE-425012 (258.00) This patch corrects the following: • Allows dtaction to properly validate passwords when using C2 Enhanced Security. • 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 469.00 OSF435CDE-015	**Patch:** Support for ISO8859-15 functionality **State:** New 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.
Patch 470.00 OSF435CDE-016	**Patch:** Fix for CDE problem with locked screen **State:** New 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.

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

Patch 471.00 OSF435DX-013	**Patch:** Fix for duplicate UID problem **State:** Supersedes patches OSF435DX-405008 (6.00), OSF435DX-425015 (40.00), OSF435DX-010 (445.00), OSF435DX-011 (446.00), OSF435DX-012 (447.00), OSF435DX-405010 (221.00), OSF435DX-009 (449.00) This patch corrects the following: • Fixes a problem where the account manager graphical interface (dxaccounts) will core dump on systems running enhanced security when performing a Find Local User... or Find NIS User... operation in which Secondary Groups is the only search criteria that has been specified. • Fixes a problem using templates for pre-expired passwords. When the administrator creates a template and within the template chooses Force Password Change at the next login, the user is not being asked to change his password as he should. • Fixes a problem where a large number of shells in /etc/shells (greater than 10) can cause dxaccounts to coredump or have unpredictable behavior. • 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). • Fixes the problem where usermod -D can coredump if an NIS group entry contains a large number of users. • Fixes a problem in which the command usermod was not allowing any commas in the comment field when the current GECOS fields were filled. • Fixes two situations in which the GUI account management program (dxaccounts) will crash in a Enhanced Security client environment when attempting to copy an NIS user account. • 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.
Patch 472.00 OSF435DX-015	**Patch:** checklist utility does not provide scroll bar **State:** New This patch fixes a problem where the checklist utility did not provide a scroll bar on higher resolution displays (1600x1200).
Patch 473.00 OSF435DX-016	**Patch:** diskconfig displays incorrectly **State:** New This patch fixes a problem where the Disk Configuration Manager application, diskconfig, displayed incorrectly on some non-Compaq X servers. The font used for menu items was incorrect so that the menus contained random symbols instead of text.

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

Patch 475.00 OSF435X11-012A	**Patch:** Xserver generates an Invalid Pixmap Error **State:** Supersedes patches OSF435X11-405010 (32.00), OSF435X11-405015A (250.00) This patch corrects the following: • Fixes the Motif tear-off menu core dump problem. The problem is seen when the tear-off menu from a pulldown menu is closed/destroyed. • Fixes a problem with Motif Drag-and-Drop where if a parent drop site was unregistered before a child drop site, subsequently unregistering the child drop site would cause a segmentation fault. • 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".
Patch 476.00 OSF435X11-014	**Patch:** Powerstorm 4D10T X server draws lines incorrectly **State:** Supersedes patches OSF435X11-004 (327.00), OSF435X11-005 (328.00), OSF435X11-006 (452.00), OSF435X11-008 (454.00) This patch corrects the following: • Fixes a problem where, on systems with a Powerstorm 4D10T (ELSA Gloria Synergy) graphics board, sometimes the graphics board was not initialized properly and failed to work on power-up or when the X server was restarted. • Fixes a problem where on systems with a Powerstorm 4D10T (ELSA Gloria Synergy) graphics board. Sometimes the X server does not draw lines correctly. • Fixes a problem where on systems with a Powerstorm 4D10T (ELSA Gloria Synergy) graphics board, sometimes the X server does not draw text correctly. This problem is seen more frequently when running under an Asian locale.
Patch 477.00 OSF435X11-015	**Patch:** Fix for Powerstorm 4D10T graphics board **State:** New This patch fixes a problem where on systems with a Powerstorm 4D10T (ELSA Gloria Synergy) graphics board. Sometimes the X server did not draw lines correctly.
Patch 478.00 OSF435X11-016A	**Patch:** Security (SSRT0547U) **State:** Supersedes patches OSF435X11-405011A (33.00), OSF435X11-009A (455.00), OSF435X11-002A (450.00), OSF435X11-003 (451.00), OSF435X11-011A (474.00) This patch corrects the following: • A potential security vulnerability has been discovered where, under certain circumstances, users may gain unauthorized access. Compaq has corrected this potential vulnerability. • Provides suppport in the X11 Environment for the Euro currency symbol using the UTF-8 Unicode locales. • Fixes various Minor System Faults (MSFs) in the X Toolkit library (libXt). • Fixes a problem in the X Display Manager (xdm) where XDMCP Indirect queries do not work. • Fixes a problem in which ^C fails to work in dtterm when logged in to a 4.0E or 4.0F system using XDMCP. • 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.

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

Patch 479.00 OSF435X11-017	**Patch:** Xlocales definitions for ISO8859-15 locales **State:** New This patch implements Xlocales definitions which 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.
Patch 485.00 OSF435-297	**Patch:** scu command panics the system **State:** New This patch fixes a panic when using the scu command. When formatting a floppy using the scu command the system panics with the following error message: System Uncorrectable Machine Check 660 (retry set)
Patch 488.00 OSF435-300A	**Patch:** Fix for AdvFS propertly list handling **State:** New This patch corrects two problems in AdvFS property list handling: • Creation of property lists entries in AdvFS filesets with no available mcells will result in kernel memory fault (kmf). • 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.
Patch 489.00 OSF435-301	**Patch:** Fix for mailsetup command **State:** New This patch fixes a problem of not completing mailsetup if the hostname ends with 0 (zero). The error message produced is: Error creating /var/adm/sendmail/.cf: exiting
Patch 491.00 OSF435-304	**Patch:** Fix for hang seen on DS10 workstations **State:** New This patch fixes a intermittent hang occurring in the I2c code. This hang is most commonly seen on the DS10 workstation.
Patch 494.00 OSF435-307	**Patch:** Fix for kernel memory fault panic **State:** New This patch fixes a problem that causes a kernel memory fault when lockmode=4 and a lock hierarchy violation is detected in the License Management Facility (LMF).
Patch 495.00 OSF435-308	**Patch:** lex command generates incorrect tables **State:** New 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 496.00 OSF435-309	**Patch:** Various fixes for ris script **State:** New This patch corrects the following problems with the /usr/sbin/ris script: • It incorrectly queried the user for a gateway to be used to serve a specific client when no gateway was required. • It could fail if no default route had been established.
Patch 503.00 OSF435-316	**Patch:** uerf command core dumps on binary errorlog files **State:** New This patch modifies uerf to not core dump on binary errorlog files with large records.

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

Patch 504.00 OSF435-317	**Patch:** Fix for FDI floppy driver **State:** New This patch fixes a problem in the FDI floppy driver. A rescursion problem causes a stack overflow resulting in the system halting for certain commands to the block device.
Patch 505.00 OSF435-319	**Patch:** Fixes a problem that occurs when using ftp **State:** New This patch fixes a problem that occurs when using ftp. When mget or nlist specify a filename with metacharacters and the mode is ASCII, the file is returned with <LF> as the end-of-file seperator. With this patch, files are returned with <CR><LF> as the end-of-file seperator.
Patch 506.00 OSF435-321	**Patch:** defragment inaccurately reports large freespace holes **State:** Supersedes patches OSF435-425429 (79.00), OSF435-196 (358.00) This patch corrects the following: • Fixes a problem with the defragment command, where the -V option is not being parsed properly. • Fixes a problem with the defragment command. Prior to this patch the defragment command could fail and display inaccurate error descriptions. The problem was caused by uninitialized variables for the command. • 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.
Patch 509.00 OSF435-324	**Patch:** verify utility corrupts filesystem **State:** Supersedes patches OSF435-070 (300.00), OSF435-093 (301.00) This patch corrects the following: • Enhances the AdvFS verify utility to detect incorrect holes in the frags file. • Enhancement for the /sbin/advfs/verify utility allows it to detect loops in the list of free frags kept in the frags file. • Avoids corruption of a filesystem when verify runs with -r and -f flags on an active domain. Verify returns usage message when -r flag is used with either -f or -d.
Patch 514.00 OSF435-329	**Patch:** news cmd fails when appending chars to file names **State:** New 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 516.00 OSF435-331	**Patch:** Fix for rpc.statd daemon hang **State:** New 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 521.00 OSF435-339	**Patch:** Support added for line continuation characters **State:** Supersedes patches OSF435-055 (111.00), OSF435-062 (116.00), OSF435-141A (308.00), OSF435-276 (427.00), OSF435-207A (368.00) This patch corrects the following: • Provides latent support for DCPI, a performance analysis tool. • Adds support for the -B symbolic option in the run-time loader. This new option to ld(1) alters the search algorithm used in symbol searches. • Provides the support needed by the Developers' Toolkit Update Kit. These updates will not install unless this patch is installed. • Fixes a problem where the linker (ld) would insert incorrect values for the symbols etext and _etext when building kernels larger than 4 MB. • Fixes the name demangling for the tools that print symbol table names generated by the C++ V6.2 compiler. This problem will only occur for most C++ objects compiled with the ANSI options. • 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.
Patch 525.00 OSF435-345	**Patch:** Fix for kernel memory fault when obtaining quota info **State:** New This patch corrects a problem that caused a kernel memory fault failure when attempting to obtain quota information on a clone file-on-file mount point.
Patch 527.00 OSF435-347	**Patch:** Correction for mkfdmn command **State:** New This patch corrects a problem that resulted in the mkfdmn command not reporting errors if you attempted to create a volume with a name that is more than 31 characters long.

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

Patch 534.00 OSF435-356	**Patch:** Security (SSRT0546U, SSRT0542U) **State:** Supersedes patches OSF435-425353 (61.00), OSF435-001A (86.00), OSF435-405520 (141.00), OSF435-087 (142.00), OSF435-116 (148.00), OSF435-156 (158.00), OSF435-405564 (242.00), OSF435-425270 (45.00), OSF435-425464 (263.00), OSF435-024A (95.00), OSF435-425387 (71.00), OSF435-129A (312.00), OSF435-130A (316.00), OSF435-205 (366.00), OSF435-221 (378.00), OSF435-227 (384.00), OSF435-234 (390.00), OSF435-245 (400.00), OSF435-425582A (320.00), OSF435-223 (379.00), OSF435-283 (433.00), OSF435-256 (408.00), OSF435-327 (512.00) This patch corrects the following: • Fixes a memory leak in the libc glob() function. • 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. • Fixes a problem in which BIND client applications are not able to resolve node names. Network applications running on a BIND client such as ping, telnet, and ftp using node names that are resolved by a BIND server will result in resolution errors such as "unknown host". • Fixes a virtual memory problem that may cause the system to panic with one of the following messages: pmap_begin_mutex_region timeout or: simple_lock timeout • Fixes a problem in libc that may cause a hang in a multithreaded process that does forking and loading of shared objects. • The routines wprintf(), swprintf(), and fwprintf() incorrectly handle the S format. Instead of treating the data as logical characters, they treat data as bytes. • Fixes a problem from a previous libc patch in which the gethostbyaddr function is not able to resolve node names. Nonstandard characters that fall out of the standard set, such as underscores, cause a node name resolution problem for the gethostbyaddr function. • Fixes a problem in which a program that is compiled with the -pthread or -threads option and the -p or -pg option will not terminate if the _exit(2) library routine is called when the program is executed. • Fixes a problem in the DECthreads library for DIGITAL UNIX. During a fork() operation, DECthreads temporarily replaces its signal-to-exception mapping for synchronous signals by installing the system default handler. This fix permits any user-installed handlers to remain in place during the fork() operation. • Fixes the following problems: – Hangs or unexpected termination of threaded processes with TotalView debugger. – gcc compiler reports errors when including header file. – A bug related to a call system FORTRAN statement.

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

Patch 534.00 continued	• Fixes a problem with the dd command in which dd aborts after a read error. This problem occurs even when the conv=noerror parameter is specified. • This patch introduces changes to the DECthreads libraries intended to improve the performance of threaded applications running on DIGITAL UNIX 4.0E. This patch specifically addresses the areas of thread scheduling, synchronization object performance, and SMP scalability. • Fixes a problem that may cause the malloc suite of functions to show heavy mutex lock contention in multithreaded applications running on multiCPU systems. • Fixes problems in the DECthreads library for DIGITAL UNIX. Included in this patch are changes to support Ladebug enhancements and a bug fix for applications that employ SCS threads of different priorities. • Fixes a problem with the wcstod system call causing a core dump. • Fixes problems with rsh(1), rlogin(1), and rcp(1) if netgroup names are defined with uppercase letters. • Fixes a problem with portmap by allowing RPC select() timeouts to occur when interrupted by signals. • Modifies the strftime() function to make the %V format specifier return the correct week. • Fixes bugs in the DECthreads library that would affect threaded applications running on DIGITAL UNIX V4.0E. The changes are related to synchronous signal processing and thread scheduling. • Fixes a problem of password error messages not being displayed during installation of the security subsystem. • Fixes a problem in which the fsck utility may be unable to repair a UFS filesystem. • Fixes and enhances the quotacheck and fsck commands. • Fixes a problem in which ufs_fsck can get blocked while attempting to flush nfs buffers for a service that has become suspended. • 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.

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

Patch 536.00 OSF435-358	**Patch:** ksh requires 2 SIGTERM signals to be sent **State:** Supersedes patches OSF435-405301 (9.00), OSF435-425344 (59.00), OSF435-425422 (78.00), OSF435-405343 (14.00), OSF435-405389 (22.00), OSF435-405479 (225.00), OSF435-405528 (232.00), OSF435-405538 (233.00), OSF435-410240 (255.00), OSF435-171 (338.00), OSF435-177 (344.00), OSF435-194 (357.00), OSF435-225 (381.00), OSF435-247 (401.00), OSF435-311 (498.00) This patch corrects the following: • Fixes a problem that was caused by the Korn shell running in EMACS mode. When a window was resized with a width that exceeded 160 characters, the next command (or even a return) would cause the ksh utility to core dump. • Corrects a problem which results in a superuser being able to inadvertently bring the system down to single user mode by accidentally killing pid 1 (init) when trying to kill a background job (%1). • Fixes a problem in the csh shell that caused a change in the way wildcard patterns were matched. The problem resulted in the error: Glob aborted - Permission denied • Fixes a problem when builtin variables (for example, TMOUT) are exported as readonly with values > 256. The set command (display all variables) will cause ksh to core dump with the error "stack overflow". • Fixes a memory management problem that occurs on systems running the Korn shell. Incorrect results occur when the length of the parameter to the echo command is altered. • Fixes a problem with /usr/bin/ksh and the named-pipe (FIFO) communication that is used by applications. • Corrects a problem that was causing ksh to core dump in vi editing mode. ksh was core dumping intermittently when using a dot (.) to repeat a command. • Fixes unexpected logouts and terminal hangups encountered when using the /bin/su command and /bin/ksh as a login shell. • ksh does a segmentation fault and core dumps when displaying a heredocument. • Fixes a core dump from ksh. • Corrects the printing of Japanese SJIS strings that are assigned to shell variables in the C shell (csh). • Corrects a problem that may cause ksh to core dump when displaying a large heredocument in a ksh script. • Fixes a problem with the Korn shell where data loss occurs when commands are piped together. • Corrects how the C shell handles 2-byte characters when running in the Japanese SJIS locale. • Fixes a problem in ksh which required 2 SIGTERM signals to be sent to the process when it exec'ed. • 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.

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

Patch 540.00 OSF435-362	**Patch:** Fixes problem with fverify creating directories **State:** New This patch fixes a problem of the fverify -n flag creating directories.
Patch 541.00 OSF435-363	**Patch:** ftp command causes system to core dump **State:** New This patch fixes a coredump problem with ftp(1) when a .netrc file contains an invalid macdef (macro definition).
Patch 543.00 OSF435-365	**Patch:** Security (SSRT0641U) **State:** New A potential security vulnerability has been discovered where, under certain circumstances users may gain unauthorized access. Compaq has corrected this potential vulnerability.

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

Patch 545.00 OSF435-367	**Patch:** Fix for vrestore command **State:** Supersedes patches OSF435-425279 (48.00), OSF435-425454 (85.00), OSF435-425470 (243.00), OSF435-425436 (82.00), OSF435-425516 (297.00), OSF435-425493 (296.00), OSF435-129D (315.00), OSF435-425582D (323.00), OSF435-219 (376.00), OSF435-281 (431.00), OSF435-323 (508.00), OSF435-343 (524.00) This patch corrects the following: • Fixes a problem with the vrestore command. The command had returned a success status code even though it had restored an incomplete file during the operation. • Fixes a problem that occurs when vrestore is run from a script. Control/c input to vrestore run from a script is not processed correctly. • Fixes the following problems with the vrestore command: – vrestore is slow to complete when a partial restore operation is requested. – vrestore fails to ignore extended attribute records for those files that are not requested in a vrestore operation. • Makes vrestore work with QIC-120 and QIC-150 tapes. • Fixes a problem with the vdump command, which was modifying the atime file attribute whenever files were backed up, which eliminated the ability to determine when the files were last accessed by a user. • Fixes a potential problem with the vdump command. • This patch introduces changes to the DECthreads libraries intended to improve the performance of threaded applications running on DIGITAL UNIX 4.0E. This patch specifically addresses the areas of thread scheduling, synchronization object performance, and SMP scalability. • Fixes problems in the DECthreads library for DIGITAL UNIX. Included in this patch are changes to support Ladebug enhancements and a bug fix for applications that employ SCS threads of different priorities. • Fixes a problem where the vdump program would dump core with the following message: nnnn Resources lost(coredump) • Fixes a problem where vdump will output the message "can't reset atime" for each file it is backing up when used with an NFS mounted file system. • The command was slow to complete when a partial restore operation was requested. • The command failed to ignore extended attribute records for the files which were not requested for a vrestore operation. • Corrects intermittent failures to display archive records for the above files (compressed or not) when the list option was selected.

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

Patch 545.00 continued	• Fixes following problems with the /sbin/vdump command: – Non-zero level dumps on links that point to a mounted file system can now be performed. – To prevent dangling links after a vrestore, directory entries are now created instead of re-creating links that points to a mount file system. – vdump no longer ignores valid nfs mounts with inodes = 5 or 4. – Fixes problem with vrestore where vrestore fails to restore certain files and directories having ACLs from a compressed vdump saveset, reporting: vrestore: error setting extended attributes 22
Patch 546.00 OSF435-368	**Patch:** volsetup script directs error output to wrong device **State:** New This patch fixes a problem in which the volsetup script directs its error output to the wrong device.
Patch 547.00 OSF435-369	**Patch:** Large binary.errlog files created in clustered env **State:** Supersedes patches OSF435-064 (163.00), OSF435-298 (486.00), OSF435-364 (542.00) This patch corrects the following: • This patch fixes a panic that occurs when KZPSA resources are not available to re-enable a channel or a device after a bus reset. The panic string is as follows: panic("(spo_process_rsp) ran out of memory!") • Fixes a problem with the KZPSA driver. A timer is not being canceled, causing a panic with the following error message: xpt_callback: callback on freed CC • Fixes a problem in which the system can panic with the following message: KZPSA PANIC SPO_RET_CARRIER:CARRIER NOT IN USE • Fixes a problem with tmv2_notify_cbf messages being logged from KPBSA adapters and creating very large binary.errlog files in a clustered environment.

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

Patch 555.00 OSF435-377	**Patch:** Fixes ITPSA, KZPCM drivers, 8951U 8952U adapters **State:** Supersedes patches OSF435-149 (157.00), OSF435-204 (365.00), OSF435-333 (518.00) This patch corrects the following: • Allows the customer to connect LVD devices to the internal connectors of an adapter that uses the ITPSA driver. It also enables full LVD functionality in the driver. • Fixes a problem that causes a deadlock condition when both SCSI channels are running, corrects a data corruption error on RZ2EA-LA and RZ2CA-LA type drives, and fixes problems with I/Os over 4 MB. • Fixes the following problems: – Problem with the ITPSA driver for KZPCM and KZPCA devices, which resulted in a synchronization problem, causing the SCSI bus to hang. – Excessive I/O command timeouts when using KZPCM on CLIPPERs causing disk I/O to be retried and fatal tape I/O errors. Additionaly the ITPSA driver now support the KZPCM, 8951U and 8952U adapters. Support has been added to identify hardware in event log. – Problem with the KZPCM driver. 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. – Several problems related to the ITPSA driver that supports the KZPCM adapter. Errors can occur while the system is processing a SCSI bus or SCSI bus device reset request that is issued from the class driver. –) Problem on the 8951U and 8952U adapters. SCSI bus resets are lost when these adapters are connected to single ended drives. • Fixes the following ITPSA driver problems: – The chip interrupt register fields in the error log are incorrect. – Lessens the opportunity of aborts being issued for an already completed I/O. – A kernel memory fault panic caused by a SWS data structure being released twice. – 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. – A lockmode 4 panic on boot.
Patch 556.00 OSF435-378	**Patch:** Fixes how libesnmp handles duplicate registrations **State:** New This patch fixes libesnmp's handling of duplicate registrations.

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

Patch 558.00 OSF435-381	**Patch:** Fix For Print Queue Problem **State:** Supersedes patches OSF435-038 (103.00), OSF435-128 (151.00), OSF435-370 (548.00) This patch corrects the following: • Includes one new print system feature for APX (which is not documented in lpd, but rather in the APX docset), and improves the overall print system. • Fixes a problem where, under certain circumstances, a print queue becomes disabled and printing stops. • Fixes the following three problems: – When printing jobs, a timeout can occur after five minutes, which causes some large print jobs to stop, and then resume printing from the beginning of the print job. – When slave lpd daemons try to process jobs on the print queue, some of them can fail to obtain a lock on the lock file, and exit with an error. – A problem where some print jobs will print out twice. • Fixes the following four problems: – A remote print job may fail to print, with the error message: lstat/open failed for dfA... no such file or directory – If a print job is printing, and the connection to the remote printer is lost, the print job does not resume printing once the connection is restored. – Sometimes, as sequence numbers wrap around from 999 to 000, job 000 gets submitted before, and prints before, job 999. – lpstat -u output is incorrect.
Patch 559.00 OSF435-382	**Patch:** Possible unaligned access fault can appear in kernel **State:** Supersedes patches OSF435-104 (144.00), OSF435-135 (153.00), OSF435-425477 (265.00), OSF435-357 (535.00), OSF435-373 (551.00) This patch corrects the following: • Fixes a kmf problem when the type of SCSI device dynamically changes. • Fixes a panic when booting with TCR 1.5 software. When system tries to initialize the ASE Availability Manager during boot, it gets a kernel memory fault. • Fixes a panic which has the following error message: lw_remove: light weight wiring(s) found • Corrects a problem in which the wrong status could be returned when using a tape device. • Fixes a problem where a possible unaligned access fault can occur in the kernel. • Fixes a problem in which the system can panic with a kernel memory fault.
Patch 562.00 OSF435-385	**Patch:** Fixes an unaligned access panic in dli_input **State:** New This patch fixes an unaligned access panic in dli_input.

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

Patch 563.00 OSF435-386	**Patch:** compress utility may not completely compress file **State:** New 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 564.00 OSF435-387	**Patch:** Shared Library Fix For AdvFS Commands **State:** Supersedes patches OSF435-074B (325.00), OSF435-226A (382.00) This patch corrects the following: • Changes the way some of the AdvFS advanced utilities work (rmvol, migrate, balance and defragment), as they were failing when trying to migrate file(s) from an AdvFS domain with heavy I/O. • Corrects a problem in AdvFS where unmounting a domain that is already in a panicked state could result in the following system panic message: log_flush_sync: pinpg error\n N1 = 5 • Fixes a problem with multivolume domains with large frag files. Verify complains about frag pages that are in sparse holes and therefore will be read as a page of zeros, causing the domain to appear as if it was corrupt.
Patch 565.00 OSF435-388A	**Patch:** Problems with voldisksetup, voldiskadd, or newfs **State:** New This patch fixes problems with voldisksetup, voldiskadd, or newfs commands. Each will report device errors while checking for overlapping partitions where there is no overlap on that particular device.
Patch 566.00 OSF435-389	**Patch:** NFS Server Fixes **State:** Supersedes patches OSF435-026 (97.00), OSF435-296 (484.00), OSF435-359 (537.00) This patch corrects the following: • Merges two corrections for the NFS server. • Fixes a system hang problem due to a bug in the nfs write gathering code. The code does not fully synch all writes. • Fixes a problem in which an NFS system using a TCP connection can crash. • Fixes a problem where nfs stale file handle errors occur on ASE clusters.
Patch 567.00 OSF435-390	**Patch:** Upgrade of Gigabit Ethernet driver to version 1.0.12 **State:** Supersedes patch OSF435-239 (394.00) This patch corrects the following: • This patch is an upgrade of the Gigabit ethernet driver to Version 1.0.8 with enhanced functionality and performance benefits. • Upgrade to the Gigabit ethernet driver Version 1.0.12 to fix various performance problems.
Patch 568.00 OSF435-391	**Patch:** Fix for update installation hang **State:** New This patch fixes a problem in which a hang can occur during update install.

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

Patch 571.00 OSF435-394	**Patch:** Fixes NetRAIN problem with HE155 (FORE) ATM cards **State:** New This patch fixes a Netrain problem when using HE155 (FORE) ATM cards. Netrain will fail when configuring LANE to join Elans.
Patch 575.00 OSF435-399	**Patch:** Fix for yppasswd **State:** New 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 577.00 OSF435-402	**Patch:** sysconfigdb incorrectly adds or deletes blank lines **State:** New This patch corrects a problem in which sysconfigdb would incorrectly add or delete blank lines to or from the target file.
Patch 578.00 OSF435-403	**Patch:** advfs showfdmn command may core dump **State:** New This patch fixes a problem in which advfs showfdmn would sometimes core dump.
Patch 580.00 OSF435-405	**Patch:** sort command aborts when running in a Japanese locale **State:** Supersedes patch OSF435-072 (165.00) This patch corrects the following: • 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. • Fixes a problem in which sort command aborts with the message: A line of the input file contains more than 20480 characters when running in a Japanese locale.
Patch 581.00 OSF435-406	**Patch:** Performance problem for round robin sequential reads **State:** Supersedes patches OSF435-405412 (26.00), OSF435-425432 (80.00) This patch corrects the following: • Fixes a problem in LSM. A data corruption occurs when readv/writev coalesced via physio while in read/writeback mode. • Corrects the following problems: – voltrace sometimes prints records out of sequence. – volsetup would fail to add disks to LSM because the volboot file is full. – vold would dump core when a user attempts to add a 257th Configuration copy to a disk group. • Fixes a performance problem for round robin sequential reads on LSM mirrored volumes.

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

Patch 582.00 OSF435-407	**Patch:** Updates sys_check utility to revision 114 **State:** Supersedes patches OSF435-065 (118.00), OSF435-073 (138.00), OSF435-366 (544.00) This patch corrects the following: • Provides bug fixes and enhancements to the sys_check utility, Version 110. • Provides bug fixes and enhancements to the sys_check utility, Version 111. • Provides a new collection information tool used by the sys_check utility. It also fixes the following two problems with the collect information tool: – A security hole where a user can become root. – Collect can not start at boot time due to incorrectly handling SIGHUP signal. • Provides the folllowing changes to the sys_check utility: – Fixes the ra200info tool from core dumping. – Updates the sys_check utility to revision 114.
Patch 583.00 OSF435-408	**Patch:** Security (SSRT0592U) **State:** Supersedes patches OSF435-405372 (19.00), OSF435-372 (550.00) This patch corrects the following: • Fixes a problem where rdist dumps core when trying to copy a partition using the rdist command. • Fixes a problem with rdist(1) which consumes huge amounts of memory, and when there are a lot of symlinks in the fileset, it can simply fail to fully populate the remote site, or cause low-memory problems on the local machine. • 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 585.00 OSF435-410	**Patch:** sendmail Core Dumps **State:** Supersedes patch OSF435-405406 (23.00) This patch corrects the following: • Fixes a problem with the sendmail program. Sendmail would dump core and not process any more jobs in the queue when it encountered control characters in a qf file. • Fixes a problem where sendmail core dumped when trying to send certain 8-bit, mime-encoded files.

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

Patch 586.00 OSF435-411A	**Patch:** Security (SSRT0588U, SSRT0642U) **State:** Supersedes patches OSF435-405349 (15.00), OSF435-425433A (81.00), OSF435-425524A (270.00), OSF435-282A (432.00), OSF435-380A (557.00) This patch corrects the following: • Resolves a problem with Enhanced Security not handling a voucher correctly from some other security mechanism such as DCE. The scenario to reproduce the problem would be: a user incorrectly enters his username at the first login: prompt, but subsequently corrects the login name when prompted again after the first failure. Without this patch, the user, upon successfully typing their login/password on the second try, would still receive the "login incorrect" message. • Resolves a problem in Enhanced Security where users could be locked out when an expiration interval was set such that it exceeded the maximum calculable date. • 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. • Fixes a problem of libsecurity producing a core file when handling error conditions. • Fixes a problem when the superuser tries to change the shell or finger information of another user when C2 Enhanced Security is installed.

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

Patch 588.00 OSF435-413	**Patch:** Various DEC C Compiler Fixes **State:** Supersedes patch OSF435-137 (154.00), OSF435-264 (415.00) This patch fixes the following problems in the DEC C compiler: • A preprocessor problem that caused whitespace differences for some (non-C) input files. This caused a problem compiling FORTRAN files. • A run-time problem when compiling using -arch ev6 in which floating-point compares were sometimes truncated to 32 bits. • A run-time problem that produced incorrect results involving a statement of type: return values[valptr–]; • A run-time problem that caused incorrect results for a large right shift. • An optimizer problem that caused incorrect results at -O2, which was discovered in the C++ compiler, but could also be a problem in C. • A run-time problem that caused a failure in the Perl op/pack test. • A compilation error for a statement of the form: a = strcpy(b,c) + 7; when compiled with -O2. • A compiler problem that allowed the generation of EV67 (CIX) instructions to be generated when using the -arch ev6 switch. • A compile time performance problem with a very large (1.6 MB) array initialization. • An optimization problem that caused incorrect output when using a signed char in a strcpy-like routine, if compiled using -O4 or higher. • An optimizer problem that caused an incorrect result for certain write-hint instructions generated when compiled with -arch ev6 -O. • A compiler crash when compiling Xemacs 21.1.4 with -O4. • An optimizer problem in loop unrolling that suppressed intermediate updates to induction variables under certain conditions. • A particular short parameter assignment caused incorrect run-time result. • An assignment of type k = (char)(l >> 8) was not sign-extended. • An optimizer problem that produced incorrect code when certain bounds checking within a loop was moved outside the loop.

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

Patch 590.00 OSF435-415	**Patch:** btcreate does not pass full pathname to newfs **State:** Supersedes patches OSF435-425391 (72.00), OSF435-305 (492.00), OSF435-360 (538.00) This patch corrects the following: • A call to the select() system call may hang or incorrectly indicate that there is a message waiting from a terminal when there is nothing there. • Fixes a problem in which the system may panic with the following error message: kernel memory fault • Corrects a problem in the btextract script which could result in the failure of the script due to a problem in the use of the grep utility in the script. • Fixes a problem that occurs when the user attemps to restore to system configured with backplane raid, btextract fails. • Fixes a problem with the btcreate command where it does not pass the full pathname to newfs.

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

Patch 591.00 OSF435-417	**Patch:** Security (SSRT0583Q, SSRT0603U, SSRT0563U) **State:** Supersedes patches OSF435-425341 (58.00), OSF435-013 (90.00), OSF435-017 (93.00), OSF435-425302 (52.00), OSF435-425324 (56.00), OSF435-425441 (83.00), OSF435-010 (87.00), OSF435-011 (88.00), OSF435-425365 (67.00), OSF435-425357 (65.00), OSF435-029 (100.00), OSF435-014 (91.00), OSF435-036 (102.00), OSF435-039 (104.00), OSF435-048 (108.00), OSF435-053 (110.00), OSF435-405328A (11.00), OSF435-020A (94.00), OSF435-025A (96.00), OSF435-068 (139.00), OSF435-080 (137.00), OSF435-405579 (177.00), OSF435-405590 (178.00), OSF435-425463 (179.00), OSF435-425467 (180.00), OSF435-425491 (181.00), OSF435-425506 (182.00), OSF435-425552 (183.00), OSF435-425569 (184.00), OSF435-047 (185.00), OSF435-103 (186.00), OSF435-108 (187.00), OSF435-112 (188.00), OSF435-114 (189.00), OSF435-120 (190.00), OSF435-122 (191.00), OSF435-123 (192.00), OSF435-124 (193.00), OSF435-140 (195.00), OSF435-144 (196.00), OSF435-145 (197.00), OSF435-146 (198.00), OSF435-015 (199.00), OSF435-152 (200.00), OSF435-155 (201.00), OSF435-157 (202.00), OSF435-042 (203.00), OSF435-052 (204.00), OSF435-083 (205.00), OSF435-085 (206.00), OSF435-006 (114.00), OSF435-092 (207.00), OSF435-425409 (259.00), OSF435-410246 (256.00), OSF435-425249A (42.00), OSF435-105 (290.00), OSF435-150A (293.00), OSF435-121 (295.00), OSF435-410219 (252.00), OSF435-113A (298.00), OSF435-151 (310.00), OSF435-110 (318.00), OSF435-079 (136.00), OSF435-163 (330.00), OSF435-172 (339.00), OSF435-192 (355.00), OSF435-193 (356.00), OSF435-206 (367.00), OSF435-209 (370.00), OSF435-213 (373.00), OSF435-215 (375.00), OSF435-224 (380.00), OSF435-228 (385.00), OSF435-240 (395.00), OSF435-243 (398.00), OSF435-244 (399.00), OSF435-251 (405.00), OSF435-252 (406.00), OSF435-253 (407.00), OSF435-261 (412.00), OSF435-266 (417.00), OSF435-267 (418.00), OSF435-275 (426.00), OSF435-277 (428.00), OSF435-160 (161.00), OSF435-284 (434.00), OSF435-170 (337.00) OSF435-405500 (227.00), OSF435-425592 (283.00), OSF435-425289 (50.00), OSF435-077A (302.00), OSF435-232A (388.00), OSF435-262 (413.00), OSF435-278 (429.00), OSF435-287 (480.00), OSF435-288 (481.00), OSF435-294 (482.00), OSF435-303 (490.00), OSF435-310 (497.00), OSF435-313 (500.00), OSF435-322 (507.00), OSF435-325 (510.00), OSF435-326 (511.00), OSF435-328 (513.00), OSF435-330 (515.00), OSF435-336 (519.00), OSF435-338 (520.00), OSF435-348 (528.00), OSF435-349 (529.00), OSF435-354 (533.00), OSF435-361 (539.00), OSF435-383 (560.00), OSF435-393 (570.00), OSF435-396 (572.00), OSF435-401 (576.00), OSF435-414 (589.00), OSF435-425494 (266.00), OSF435-424 (593.00), OSF435-332A (517.00), OSF435-346 (526.00), OSF435-374A (552.00), OSF435-353A (532.00), OSF435-003 (101.00), OSF435-004 (105.00), OSF435-089 (143.00), OSF435-118 (149.00), OSF435-127 (150.00), OSF435-165 (332.00), OSF435-167 (334.00), OSF435-138 (155.00), OSF435-174 (341.00), OSF435-340 (522.00), OSF435-371 (549.00), OSF435-398 (574.00), OSF435-241 (396.00), OSF435-412 (587.00)

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

Patch 591.00 continued	• Fixes a problem when a processor is commanded to stop during a heavy load but does not actually halt. • Fixes a problem when a setuid program is exec'ed, and the error message "privileges disabled because of outstanding IPC access to task" is issued. • Corrects a potential boot panic problem by limiting the size of the bufcache. • This patch fixes the following two problems that occur on an NFS file server using a Network Appliance server: – New files may not be listed in directory reads. For example, when the ls command is used not all the files may be listed. – When a directory listing is requested from a Network Appliance server, more data than was requested may be returned and the extra data is lost by the DIGITAL UNIX client. The problem can be seen by entering the ls command; not all the files on the server are listed. • A flaw in NFS client operation can result in a KMF panic. • Fixes a problem where a user application may receive an EIO error back from an fsync() call. • A message size of zero passed to msgsnd() can result in a kernel memory fault panic. • Corrects a performance problem with POSIX timers. • Avoids a "kernel memory fault" panic from sigsgdisp(). The problem has only been seen when shutting down an Oracle database. • Corrects performance related problems. A system running low on free memory or showing heavy pagein activity will need this patch. • Corrects a small accounting problem where the measured time for a process was an integral rather than mean value. • Fixes several problems in AdvFS.

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

Patch 591.00 continued	• Includes several corrections for AdvFS, ufs, and vfs. • This patch must be installed to allow the X.25 WAN layered product to run on DIGITAL UNIX V4.0E. • Corrects a system performance problem on a freshly booted AlphaServer 4000 and similar systems. • Fixes a routing corruption that could been seen as a kernel memory fault or a corruption within the 128-byte kernel memory bucket. • Corrects a problem where incorrect NFS client locking caused a KFM panic. • Fixes a problem where NFS clients may hang in the uninterruptable state. • Fixes a problem in which the msleep() syscall was not marked as a cancellation point. This problem occurred only if your C programs were complied using the -pthread switch. • Fixes a problem that can cause an NFS client application to hang, or causes a "lock already owned by thread" panic when lockmode equals 4. • Fixes a problem with RPC where heavy traffic (such as mail over NFS) may cause performance problems. • Fixes a problem with poor performance of NFS/UDP over a GigaBit Ethernet network interface (DEGPA). • Fixes a rare problem in the NFS subsystem in which a "kernel memory fault" panic will be seen originating from the free() routine either when the NFS server daemon (nfsd) is processing a request or is shut down. • Fixes problems with sqrt instruction emulation and a rare rounding problem with denormalized values. • Fixes a problem where the system crashes with the following error message: lw_remove: light weight wiring(s) found • Fixes a problem that causes a panic to occur at boot time if the system has a large boot time memory requirement and only a portion of memory has been tested. • Fixes a deadlock that can occur when a thread is in sigwaitprim(), and a second signal in the sigwait set is being delievered. An example stack from of the sigwait thread is: simple_lock_time_violation() mpsleep() sigwaitprim() syscall() _Xsyscall() And the delivering threads stack would be: psignal_internal() kill() syscall() _Xsyscall() • Fixes a problem in the subsystem configuration bootstrap process where a status variable might not get initialized correctly and therefore subsequent entries from /etc/sysconfigtab might not get set correctly. • Corrects a "simple_lock: time limit exceeded" panic in softclock_scan().

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

Patch 591.00 continued	• Fixes a panic which has the following error message: simple_lock: time limit exceeded • Fixes an LMF license problem where LMF fails to decrement the OSF-USR license when xdm is selected as the default window manager. • Fixes problems with sqrt instruction emulation when operating on IEEE signaling NaNs or other IEEE special values. • Fixes a problem where a network hang can occur because the network isr thread is not running at realtime priority. As a result, some of the realtime daemons or user programs may preempt the netisr thread and hang network activity. • 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. • Fixes a performance problem associated with page coloring for realtime applications (rt_preempt_opt=1). There is a new tuneable, vm_page_color_private, which is modified in the vm section of the sysconfigtab file. The default value for this variable is 0, so to enable this feature the variable must be set to 1. • Corrects a problem where a signal is delivered, but not responded to by the target process. • Fixes a problem in which sem_wait() does not get interrupted by a SIGCHLD signal if the program is compiled/linked with -pthread. • Changes the behavior of mlockall() to make a process unswappable. • Fixes a panic of "get_color_bucket: empty buckets" when the sysconfig attribute private-cache-percent is nonzero. • Fixes a prior regression that prevented full crash dumps from working properly. • Fixes several problems in the kernel: – A panic with the message vm_unwire: page is not wired. – A panic with the message kernel_object_bad: bad operation. – A system hang due to deadlock between the swapin thread and ps both accessing the same task. • Provides functionality to allow the detection of unlinked referenced files. This is to assist customers in recovering disk space. • Fixes a problem in which the kernel misses profiling samples for multithreaded applications that are implemented to use system contention scope (SCS) threads.

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

Patch 591.00 continued	• In multithreaded programs, the fork() system call was failing to preserve the floating-point state. • Fixes a system hang caused by an infinite loop with out-of-band networking data. • Fixes a problem where NFS does not update mtime and atime for special files and named pipes. • Fixes a kernel problem, where proper locking/reference count management was not being performed. This could result in a "lock-terminate: lock held" system panic. • Fixes a panic with the following panic string: pgmv: session leader attempted setp • Fixes a kernel memory fault caused by a streams SMP race condition. • Fixes a problem that occurs on AdvFS systems. The system will panic with the following error message: malloc_overflow: guard space corruption • Fixes a problem where several processes accessing the same AdvFS file can hang in ubc_lookup(). • Fixes an kernel memory fault caused by a streams SMP race condition. • Fixes a problem where a system panic will occur when accessing an ISO9660 format CDROM. • Fixes the following problems: – A kernel memory fault system panic in the spec_reclaim routine. – When executing the file command against a lat (BSD) special device, the file process will hang. – On multiCPU systems, hangs can occur in the revoke system call when multiple threads attempt to call evoke at the same time. • Fixes a problem where process accounting data was not written to the accounting file when it was on an NFS-mounted file system. This problem occurred on Dataless Management Services (DMS) client systems. • When a thread issues a resume request against another thread before it has actually suspended, the target thread is incorrectly suspended. At times it may suspend indefinitely.

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

Patch 591.00 continued	• nxm_get_state() system call did not return a failure status if a target thread is not blocked at the time the call is executed. • Provides platform support for software interleaving on the AlphaServer 4000 family of platforms. • Supports two new DMA driver function prototypes that were added in V4.0F; dma_get_num_val_sgentrys() and dma_get_sgentry_reset(). These functions provide source and binary compatibility across Y2K-compliant versions of DIGITAL/Tru64 UNIX. • Fixes a kernel memory fault from socket code. The kernel memory fault results from failing to get a lock on a list of threads that have requested resources on a socket. • Fixes a system hang in which there is a large number of pending ioctls on the streams queue. • Fixes a problem that causes system panics when thread_swappable is called with the current_thread as the target thread, when the thread is about to be swapped out. • Fixes a problem with the map entry indexing scheme that results in the following panic: pmap_release_page: page not found • Fixes a restart detection problem with the proplistd daemon. Prior to this fix, when mounting a relocated ASE NFS service with property lists, clients did not detect that the proplistd RPC port number had changed. Clients continued to use the proplistd RPC port number of the old ASE cluster member. • Fixes a problem in which certain invalid kernel address ranges may get ignored. This can result in invalid kernel memory accesses to be left unnoticed. • 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. • Fixes a problem with CDFS. Data corruption occurs when reading beyond the end of a partition. • Fixes a problem in the module core() that can cause a panic with the message: vrele: bad ref count • Fixes two separate problems: – A panic in the kernel with the following error message: simple_lock: time limit exceeded – A panic occurs when booting kernel interactively and setting the memlimit. The panic error message is as follows: kernel memory fault • Fixes a UFS file system panic with the following error message: malloc_check_checksum: memory pool corruption • Improves UFS performance by no longer prematurely writing single pages.

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

Patch 591.00 continued	• Fixes system crashes seen on ASE or cluster systems when changing the network interfaces. The stack is not informative and the panic may be "trap: illegal instruction," or "kernel memory fault." • 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. • Applications using fcntl() system calls may appear to hang. • Fixes "simple_lock: time limit exceeded" panics. • Patch for a Compaq AlphaServer DS20. A fix has been made to the handling of power supply, temperature, and fan events. • Fixes an nfs/ufs/vm deadlock. While serving a client, the system running ASE/DT as an NFS server can hang with deadlock. • Fixes a problem in which the system may panic with the error message "kernel memory fault". • Fixes two problems; fork can fail to obtain swap space, and the resource limitation on core files does not work as documented. • Fixes a system hang condition. All NFS-related services may deadlock. • Fixes a problem where the system can panic with the console message: bs_bf_htop: invalid handle\n N1 = 0 • Fixes the following problems: – A system panic, with panic the string "simple_lock_terminate: lock busy". – A system panic, with panic the string "lock_terminate: lock held". – Removes the restriction of the maximum number of threads allowed systemwide. • Fixes a problem with kdbx. A core file created by kdbx was left in the root directory when recovering from a system crash. • Fixes a problem in mountd. The NFS server allows read/write access to clients not on the exports list and other clients to be incorrectly denied access. • Fixes a problem in mountd where multiple A records in DNS database for an NFS client will not always succeed. • Adds automatic detection of a cdfs file system for the mount(8) command. • Fixes a problem with the mount command where it sometimes kills other processes. • Fixes a problem in which mount would incorrectly fall back to Version 2 after certain errors had been encountered using Version 3. • Fixes a system pause seen when doing a lot of I/O to UFS filesystems.

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

Patch 591.00 continued	• This patch fixes a problem in which the vmstat -M command incorrectly matches bucket numbers and bucket indices. • Fixes a system panic on multi-process systems (approximately 12 cpus) with large memory (128GB). The system can panic with: panic: lock time on vm_page_free_lock • Fixes a problem where the system can panic with the panic string ;secsize_resid < d_reclen' when accessing a defective cdrom. • Fixes a problem where partitioned turbolasers return incorrect cpu data for CPUs that are not in the partition. • Fixes a problem where ubc_msync() may not flush out all the pages in the requested range. • Fixes var adm messages from truncation on larger configurations by raising the default size (4096) of msgbuf_size to 8192. • Fixes a problem where systems with the BL13 patch kit installed would run low on kernel memory after process accounting had been running for a while. • Fixes the AdvFS race between extending and reading subextent maps and avoids the panic occured in advfs bs_get_bf_xtnt_map code. This patch also fixes the race with removing storage causing kernel memory fault. • Fixes a problem that could result in a incorrect scheduling of threads when they were dispatched from the idle state. • 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. • Fixes a panic in AdvFS which can have the following error messages: panic (cpu 1): bs_cow_pg: pin clone err or panic (cpu 1): bs_cow_pg: cannot get blkMap • Fixes a kernel memory fault caused by a mishandling of multicast addresses on the FDDI interface. • A correction to the port allocation code now prevents a user from allocating port zero if ipport_userreserved is set to 65535. • Fixes a problem where DIGITAL UNIX systems may panic with one of the following strings while attempting to unlock a socket: Unaligned kernel space access from kernel mode or kernel memory fault • Fixes a problem where resets are seen due to proxy packets getting into the ipintrcacheaddr cache. • Fix for AOL systems running Inktomi code. It provides enabling hooks for Inktomi caching server code. • Fixes a kernel memory fault and an SMP race condition with the AltaVista Firewall 98 server on a multi-CPU system.

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

Patch 591.00 continued	• Fixes a problem when a default IP address and a cluster virtual IP address get interchanged after a network restart. The default interface address is used by all outgoing traffic and the alias address is only usable for the incoming packets. • Fixes a problem on systems running screend where TCP/IP fragments are being dropped. • Fixes a problem where RCP commands issued from a Sun Solaris system to DIGITAL/Tru64 UNIX may sometimes fail incorrectly with the error message: Connection reset by peer • Fixes a TCP performance problem if the TCP window scale option is turned off when using the HIPPI interface. • Fixes a system panic: tcphdr too big • Consists of changes necessary for AV firewall 98 to pass ICSA certification. • Involves virtual mac addressing.

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

Patch 594.00 OSF435-435	**Patch:** Fix for Powerstorm 4D10T **State:** Supersedes patches OSF435-028 (99.00), OSF435-425378 (69.00), OSF435-061 (115.00), OSF435-158 (159.00), OSF435-071 (164.00), OSF435-217 (326.00), OSF435-216 (329.00), OSF435-182 (348.00), OSF435-229 (386.00), OSF435-233 (389.00), OSF435-295 (483.00), OSF435-342 (523.00), OSF435-375 (553.00), OSF435-376 (554.00), OSF435-397 (573.00), OSF435-404 (579.00) This patch corrects the following: • Fixes the following problems that may occur when using QLogic adapters: – Fixes "simple_lock: time limit exceeded" panics. – Fixes a problem in which adapter errors are reported as disk errors. – Fixes a problem in which a processor may appear to hang for long periods of time when doing large, nonaligned, nonblock, multiple I/O transfers. – Fixes a problem in which random memory corruption problems may occur when a device error is encountered and the device does not have an entry in the DDR database. • Fixes three separate problems as follows: – Fixes a problem in the CAM driver. A disk failure can cause the driver to spend too much time retrying interleaved Test Unit Ready and Start Unit commands. As a result, the logging of the hard error caused by the disk failure is delayed. – Fixes a problem with the ddr_config command, where the -x option would intermittently fail. – Implements the READ POSITION and LOCATE commands in the tape driver. Added new ioctl MTIOCRDPOS and new MTSEEK and MTSEEKDS subcommands to MTIOCTOP. • Enables LVD support for the Intraserver 895/896 controllers. It also enables them to be the only SCSI controller in a system. • Fixes the problem that causes a "ccmn_rem_ccb3: ccb not on any list" panic and a device starvation problem when Rapid Error Recovery is in use. • Fixes the erroneous SAR Stats implementation of CAM statistics. The original CAM stat's macros calculated inappropriate time deltas because they were not measured on a per-I/O basis, and the times did not account for overlapping I/O. • Fixes various problems with the driver support for the Powerstorm 4D10T (ELSA Gloria Synergy) graphics board. • Provides support for the DAPCA HE622 ATM adapter. • Fixes two problems: – Callback thread blocking forever in isp_enable_lun – assert wait in xpt_ccb_alloc panic • Fixes the problem where the tapex -L command would report failure when run on certain devices. The failure would be reported when the command was run on certain TLZ09 devices, depending on the firmware.

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

Patch 594.00 continued	• Fixes a problem with the CDFS file system. The default "a" partitions are being made incorrectly by the disk driver for ISO-9660 CDs causing data corruption when reading beyond the end of the partition. Only new and non-DEC CD-ROM drives are affected. • Fix to prevent I/O stalling infinitely when ccb queue on a device is full. • Updates the lfa ATM driver to V1.0.16 and fixes the following two ATM driver problems: – Fixes a soft hang that can occur when running NFS over ATM. – Allows the ATM subsystem to be shut down successfully in the event of a board hang. • Fixes a problem on configurations having multiple Qlogic 1020/1040 based SCSI controllers (for example KZPBAs) and multiple CPUs. The problem could result in stalled I/O. This could be seen as a performance degradation, command timeouts, or in the worse cases a system hang condition. • Fixes a problem which could result in unit attention status being missed. • Fixes a problem where on systems with a Powerstorm 4D10T (ELSA Gloria Synergy) graphics board, the graphics were not reset to console mode (the blue screen) when the halt button was pressed. • Fixes callback on freed CCB panics. • Fixes problems with the following: – Continuous resets when an I/O command is causing the resets. – Read capacity recovery failure. – Bad block replacement (BBR) processing.
Patch 596.00 OSF435X11-012B	**Patch:** Fixes a problem with the toggle button **State:** Supersedes patch OSF435X11-40501B (251.00) This patch corrects the following: • Fixes a problem with Motif Drag-and-Drop where, if a parent drop site was unregistered before a child drop site, subsequently unregistering the child drop site would cause a segmentation fault. • 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" message.

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

Patch 597.00 OSF435X11-016B	**Patch:** Security (SSRT0547U) **State:** Supersedes patches OSF435X11-405011B (124.00), OSF435X11-009C (461.00), OSF435X11-002B (463.00), OSF435X11-011B (595.00) This patch corrects the following: • A potential security vulnerability has been discovered where, under certain circumstances, users may gain unauthorized access. Compaq has corrected this potential vulnerability. • Provides suppport in the X11 Environment for the Euro currency symbol using the UTF-8 Unicode locales. • Fixes various Minor System Faults (MSFs) in the X Toolkit library (libXt). • Fixes a problem in which ^C fails to work in dtterm when logged in to a 4.0E or 4.0F system using XDMCP. • 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.
Patch 599.00 OSF435-300C	**Patch:** Creating property list entries results in kmf **State:** New This patch corrects two problems in AdvFS property list handling: • Creation of property lists entries in AdvFS filesets with no available mcells will result in kernel memory fault (kmf). • 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.
Patch 603.00 OSF435-388B	**Patch:** voldisksetup reports errors when checking partitions **State:** New This patch fixes problems with voldisksetup, voldiskadd, or newfs commands. Each will report device errors while checking for overlapping partitions where there is no overlap on that particular device.

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

Patch 604.00 OSF435-353B	**Patch:** Fixes AdvFS race between extending and reading maps **State:** Supersedes patches OSF435-425257 (44.00), OSF435-425249B (126.00), OSF435-020B (131.00), OSF435-025B (132.00), OSF435-425513 (208.00), OSF435-100 (209.00), OSF435-111 (210.00), OSF435-119 (211.00), OSF435-126 (212.00), OSF435-134 (213.00), OSF435-143 (214.00), OSF435-148 (215.00), OSF435-066 (216.00), OSF435-067 (217.00), OSF435-074 (218.00), OSF435-081 (219.00), OSF435-058 (113.00), OSF435-094 (220.00), OSF435-150B (294.00), OSF435-190 (353.00), OSF435-191 (354.00), OSF435-197 (359.00), OSF435-210 (371.00), OSF435-242 (397.00), OSF435-257 (409.00), OSF435-259 (411.00), OSF435-268 (419.00), OSF435-271 (422.00), OSF435-113B (299.00), OSF435-274 (425.00),OSF435-299 (487.00), OSF435-306 (493.00), OSF435-312 (499.00), OSF435-314 (501.00), OSF435-315 (502.00), OSF435-350 (530.00), OSF435-352 (531.00), OSF435-384 (561.00), OSF435-392 (569.00), OSF435-409 (584.00), OSF435-226B (383.00), OSF435-422 (592.00), OSF435-300B (598.00), OSF435-332B (600.00), OSF435-374B (601.00) This patch corrects the following: • Fixes a problem with AdvFS in which the following panic occurs: clone: str_stripe_clone err • Fixes a problem that occurs on AdvFS systems. The system will panic with the following error message: malloc_overflow: guard space corruption • Fixes several problems in AdvFS. • Includes several corrections for AdvFS, ufs, and vfs. • Corrects an AdvFS hang. • Fixes a problem where a system can panic with a kernel memory fault in overlay_xtnt_map() when any of the AdvFS migration utilities (migrate, balance, rmvol, or defragment) are run on an AdvFS domain. • Fixes a problem in which a system using AdvFS can Kernel Memory Fault when truncating a frag file for a fileset that is not mounted. • Fixes a problem in which a system can hang because cleanup_closed_list() can go into a loop. • Fixes a problem in which the update daemon can hang. • Fixes a problem with AdvFS that will cause the system to panic with "kernel memory fault" in audit_rec_build(). • Fixes a problem where the statfs system call was reporting incorrect block usage on AdvFS filesets. As a side effect of this problem, the sendmail utility may sleep needlessly waiting for space to become available. • Fixes an AdvFS Domain Panic that occurs with the following message on the console: load_x_cache: bad status from bs_refpg of sbm • Fixes a problem on systems using the AdvFS filesystem, where the system can panic with the panic string: del_clean_mcell_list: no primary xtnt record

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

Patch 604.00 continued	• Fixes the following problems: – A potential system hang when inactivating an AdvFS domain (QAR 65739). – A potential problem during AdvFS domain activation that can cause an AdvFS domain to be unmountable (QAR 64945). • Fixes a panic in the AdvFS system. The panic has the following error message: lock_read: hierarchy violation • Changes the way some of the AdvFS advanced utilities work (rmvol, migrate, balance, and defragment) as they were failing when trying to migrate file(s) from an AdvFS domain with heavy I/O. • Applies to AdvFS use only and corrects a problem in which rmvol(8) will not remove multiple stripes of the same file on a volume. The error code EBAD_VDI (-1030) may be displayed. • Provides the following fixes and enhancements to AdvFS: – AdvFS volumes were not setting the default I/O byte transfer size to the preferred size reported by the disk drives. – AdvFS chvol read and write transfer size range was increased. – The read-ahead algorithm was modified to improve performance under certain conditions. – Fixes a problem where several processes accessing the same AdvFS file can hang in ubc_lookup(). – Fixes the following problems: ☐ A kernel memory fault system panic in routine spec_reclaim. ☐ When executing the file command against a lat (BSD) special device, the file process will hang. ☐ On multiCPU systems, hangs can occur in the revoke system call when multiple threads attempt to call revoke at the same time. – Fixes a problem that caused the system to hang when AdvFS tests were run in lockmode 4. The fix allows xfer_xtnts_to_clone to recover after a crash. • Fixes a problem with the AdvFS addvol command. Prior to this patch, if the advol command was interrupted and a second addvol command was run, the AdvFS domain would be rendered unusable. • Fixes a problem that caused AdvFS system panics with a lock hierarchy violation. • Corrects a problem in AdvFS that causes single-CPU systems to hang and causes multiple-CPU systems to panic with a "simple lock time limit exceeded" error specifying lock class name BfAccessTblMutex.

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

Patch 604.00 continued	• Fixes the problem where the system panics if AdvFS detects an inconsistency in the free list of mcells that is kept on a per-volume basis in an AdvFS domain. The panic string seen with this panic follows: alloc_mcell: bad mcell free list • Fixes a problem where update takes too long to sync mmap files when using an AdvFS file system. • Fixes the potential directory corruption when a system crashes during rmdir. • Fixes the problem where the system panics whenever nextFlushSeq reaches the max. This fix allows nextFlushSeq (and other lsn buffers) to roll over. • Fixes the following two problems in AdvFS: – When a "log half full" or "log full" problem occurs, an entire system will panic. – The erorr message "ftx_bfdmn_recovery:bad record size\n N1 = 1" is received when the wordCnt, as returned by lgr_read, is not enough to hold the ftxDoneLRT record that preceeds each log record in a log page. – Fixes the AdvFS race between extending and reading subextent maps and avoids the panic that occured in AdvFS bs_get_bf_xtnt_map code. This patch also fixes the race with removing storage causing a kernel memory fault. – 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. – Fixes a panic in AdvFS which can have the following error messages: panic (cpu 1): bs_cow_pg: pin clone err or panic (cpu 1): bs_cow_pg: cannot get blkMap

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

Patch 604.00 continued	•
	• Corrects a problem where a "can't clear a bit twice" panic occurs after an unanticipated system crash and an improperly handled AdvFS recovery operation.
	• Corrects a problem in AdvFS where unmounting a domain that is already in a panicked state could result in the following system panic message: log_flush_sync: pinpg error\n N1 = 5
	• Fixes a problem in AdvFS. AdvFS may skip filesystem recovery after aborted domain activation.
	• Fixes a problem in AdvFS. The system panics with the following error message: SMP Assertion failed
	• Corrects a kernel memory fault that occurs when entering the mount -o dual command. Abbreviated stack: 9 _XentMM() 10 bs_bfdmn_sweep() 11 bs_bfdmn_activate() 12 bs_bfdmn_tbl_activate() 13 bs_bfset_activate_int() 14 bs_bfset_activate() 15 advfs_mountfs()
	• Fixes a problem in which it prevents a system panic if str_stripe_clone returns an error.
	• Fixes a problem where the close_one_int() function enables the MIGTRUNC lock unnecessarily.
	• Fixes a problem that may cause panics to occur when msfs_getpage() receives an error return from fs_write_add_stg() when attempting to write to an AdvFS domain that is out of disk space.
	• Fixes a problem in AdvFS. A fileset is busy when attempting to unmount giving an EBUSY error even though the fileset has no open files.
	• Fixes a problem in the AdvFS system. A panic occurs with the following error message: lock_read: hierarchy violation
	• Fixes a situation in which a slight memory leak can occur when recovering Advfs domains with mount.
	• Fixes a problem where a single CPU system using AdvFS can hang in cleanup_closed_list().
	• Corrects AdvFS problems involving clone filesets. The statfs syscall (used by df) was incorrectly returning zero blocks USED for clones. The read-ahead code was incorrectly passing up opportunities to do read-ahead on clone filesets, resulting in a large performance penalty.
	• Corrects two problems in AdvFS property list handling: – Creation of property lists entries in AdvFS filesets with no available mcells will result in kernel memory fault (kmf). – 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.

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

Patch 605.00 OSF435-411B	**Patch:** Security (SSRT0588U, SSRT0642U) **State:** Supersedes patches OSF435-425433B (128.00), OSF435-425524B (271.00), OSF435-282B (459.00), OSF435-380B (602.00) This patch corrects the following: • Resolves a problem in Enhanced Security where users could be locked out when an expiration interval was set such that it exceeded the maximum calculable date. • 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. • Fixes a problem of libsecurity producing a core file when handling error conditions. • Fixes a problem when the superuser tries to change the shell or finger information of another user when C2 Enhanced Security is installed.

3

Summary of TruCluster Software Patches

This chapter summarizes the TruCluster software patches included in Patch Kit-0004.

Table 3–1 lists patches that have been updated.

Table 3–2 provides a summary of patches.

Table 3–1: Updated TruCluster Software Patches

Patch IDs	Change Summary
Patches 1.00, 31.00, 19.00, 24.00, 26.00, 64.00, 76.00, 90.00	Superseded by Patch 83.00
Patches 14.00, 20.00, 23.00, 37.00, 50.00, 5.00, 66.00, 71.00	Superseded by Patch 86.00
Patches 2.00, 8.00, 10.00, 15.00, 16.00, 18.00, 21.00, 22.01, 38.00, 30.00, 44.00, 53.00, 56.00, 4.00, 45.00, 62.00, 51.00, 69.00, 67.00, 73.00, 72.00, 74.00, 75.00, 81.00, 82.00, 84.00, 85.00, 87.00, 88.00, 89.00	Superseded by Patch 91.00
Patches 2.00, 8.00, 10.00, 15.00, 16.00, 18.00, 21.00, 22.01, 33.00, 40.00, 57.00, 63.00, 68.00, 77.0, 78.00, 80.00, 92.00, 93.00, 94.00	Superseded by Patch 95.00

Table 3–2: Summary of TruCluster Patches

Patch IDs	Abstract
Patch 11.00 TCR150-012	**Patch:** Cluster Map Not Being Loaded At Boot Time Correction **State:** Existing Fixes a problem in TruCluster Available Server V1.5. The cluster map (/etc/CCM) was not being loaded at boot time, which prevented the Cluster Monitor utility (cmon) and its associated daemons (tractd and submon) from running.
Patch 13.00 TCR150DX-003	**Patch:** Cluster Monitor Hang Correction **State:** Existing Fixes a problem where if the name of an ASE service is changed using asemgr, any Cluster Monitor (cmon) that is running on the cluster will hang.
Patch 28.00 TCR150-031	**Patch:** ASE Check Service Script Could Be Corrupt **State:** Existing This patch corrects a problem in which an ASE check service script could become corrupted in the ASE configuration data base.

Table 3–2: Summary of TruCluster Patches (cont.)

Patch 36.00 TCR150-025-1	**Patch:** dlm_panic Fix **State:** Supersedes patches TCR150-016 (14.00), TCR150-022 (20.00), TCR150-025 (23.00) This patch fixes the following problems: • Problem that can cause a cluster member to panic in rcv_deqlk_msg() with the panic string set to: dlm_panic • Provides performance enhancements that are required by Oracle V8.0.5. • Fixes a system panic with the following message: snd_grantlk_msg: no memory for message
Patch 46.00 TCR150-042	**Patch:** LSM Disk Not Updated in ASE Database **State:** Supersedes patches TCR150-014 (12.00), TCR150-027 (25.00), TCR150-027A-1 (34.01), TCR150-035 (43.00) This patch fixes the following problems: • Provides support in asemgr for the new AdvFS mount option -o noatimes. • Fixes a problem in which, under certain circumstances, an ASE service modification could result in a corrupted configuration data base. • Fixes a problem in which a service fails to start when the ASE service name and the AdvFS domain name are identical. • Fixes a problem where LSM disk information was not properly updated in the ASE database when volumes were removed from a disk service. • Fixes a deadlock condition between the DLM rebuild thread and the Connection Manager ping daemon (cnxpingd). The deadlock can cause users of DLM (e.g., Oracle) to hang.
Patch 47.00 TCR150-044	**Patch:** Kernel Memory Fault Panic **State:** Existing This patch fixes two panics: • A kernel memory fault with bss_rm_biodone() in the stack. • A "bsc_rm_strategy: can't send notification" panic.
Patch 48.00 TCR150-045	**Patch:** Fix for AdvFS Panic **State:** Supersedes patch TCR150-008 (7.00) This patch corrects the following: • Fixes a problem in which running the vquotacheck command on a filesystem participating in an ASE service will cause a system to panic if the service fails over or relocates while the command is in progress. • Fixes a problem that could cause an AdvFS panic when a service that has quotas enabled is relocated. The problem occurs if a command is running that has a large number of arguments (>99).

Table 3–2: Summary of TruCluster Patches (cont.)

Patch 49.00 TCR150-046	**Patch:** drdadmin Incorrectly Builds drdtab File **State:** Supersedes patch TCR150-007 (6.00) This patch fixes the following problems: • If a cluster member issued a drdadmin command to create new DRD map entry while another member is rebooting or had explicitly issued a SCSI bus reset, the command may fail with the following message: drdadmin: Error: Can not add map entry for drdadmin: Error: Can not add map entry for <drd device name> • During system startup, as each DRD map entry is being added. the following informational message may be seen on the console: No cluster has been setup, there are 0 nodes. • Fixes a problem where drdadmin does not properly build the drdtab file during bootup.
Patch 52.00 TCR150-050	**Patch:** Adding second cnxmond Causes Cluster Partition **State:** Existing This patch fixes a problem where starting a second cnxmond could cause a cluster partition. Attempting to start a second one will now log an error message, and the new process will exit.
Patch 60.00 TCR150-040A	**Patch:** Fix for Memory Channel API **State:** Supersedes patches TCR150-010 (9.00), TCR150-019 (17.00), TCR150-019-1 (41.00), TCR150-039A (58.00) This patch fixes the following problems: • Problem with the Memory Channel API whereby the function imc_asalloc did not allow a negative key (most significant bit of key being set). • Problem that caused mcm_init to core dump when resolver fails on system boot. • Problem in which a resolver failure produces an unhelpful error message from mcm_init on boot. • Problem with the Memory Channel API whereby the function imc_ckerrcnt was signifying an error had occured when in fact no error had occurred. The following is the error code seen when running an MPI code: [5]MPI Die-ump2chck.c 91 "ump_wait failure" (-16)
Patch 61.00 TCR150-040B	**Patch:** Fix For ump_wait failure Error **State:** Supersedes patches TCR150-010 (9.00), TCR150-019 (17.00), TCR150-019B (42.00), TCR150-039B (59.00) This patch fixes the following problems: • Problem with the Memory Channel API whereby the function imc_asalloc did not allow a negative key (most significant bit of key being set). • Problem that caused mcm_init to core dump when resolver fails on system boot. • Fixes a problem in which a resolver failure produces an unhelpful error message from mcm_init on boot. • Fixes a problem with the Memory Channel API whereby the function imc_ckerrcnt was signifying an error had occured when in fact no error had occurred. The following is the error code seen when running an MPI code: [5]MPI Die-ump2chck.c 91 "ump_wait failure" (-16)

Table 3–2: Summary of TruCluster Patches (cont.)

Patch 65.00 TCR150-006B	**Patch:** System Panic dlm getch: illegal csid Correction **State:** Existing Fixes a problem in the TruCluster Production Server Software in which a system can panic with the following message: dlm getch: illegal csid
Patch 70.00 TCR150-057	**Patch:** Fix For tmv2_notify_cbf Error Message **State:** Supersedes patches TCR150-004 (3.00), TCR150-030 (27.00), TCR150-036 (32.00) This patch fixes the following problems in the ASE Availability Manager (AM): • A "simple_lock: time limit exceeded" panic on multiprocessor and system hangs in single processor systems. This can occur when multiple host target mode requests are issued due to SCSI aborts and resets on a shared bus. • A kernel memory fault panic caused by a race condition when the AM de-initializes. • Fixes a problem in which tape services may not failover as expected. • Fixes two problems: – A problem in which the following messages may appear in the binary error log: SCSI STATUS RESERVATION CONFLICT Target xx Lun xx or: Max SEND SCSI BUSY retries exhausted – A problem in which a system may panic if the system has an IDE interface and ASE is then installed. • Fixes a problem in clustered systems. It reduces the occurrences of tmv2_notify_cbf error messages in the errlog.

Table 3–2: Summary of TruCluster Patches (cont.)

Patch 79.00 TCR150-062C	**Patch:** Message Service Routine Fixes **State:** Supersedes patches TCR150-003 (2.00), TCR150-009 (8.00), TCR150-011 (10.00), TCR150-017 (15.00), TCR150-018 (16.00), TCR150-020 (18.00), TCR150-023 (21.00), TCR150-024-1 (22.01), TCR150-014 (12.00), TCR150-027 (25.00), TCR150-024B-1 (39.00), TCR150-027B-1 (35.01) This patch fixes the following problems: • Fixes a problem in the message service routines used by the daemons in TruCluster Available Server and TruCluster Production Server software. When the message queue fills, the following message is entered in the daemon.log file, but the queue is not emptied: msgSvc: message queue overflow, LOST MESSAGE! From this point on, no further messages will be received. • Fixes a problem in Version 1.5 of the TruCluster Production Server and TruClusterAvailable Server products where, during the start of a service, missing special device files were not being created for HSZ disks. Since the special device files did not get created, the service start would fail. • Fixes a segmentation fault that can cause ASE daemons to exit or hang. • Fixes a problem where the Host Status Monitor (asehsm) incorrectly reports a network down (HSM_NI_STATUS DOWN) if the counters for the network interface get zeroed. • Fixes a problem that caused the asedirector to core dump if asemgr processes were modifying services from more than one node in the cluster at the same time. • Fixes scalability problems in the DECsafe Available Server, TruCluster Available Server, and TruCluster Production Server products. The problems caused the asemgr to core dump when adding or modifying services with a large number of disks. • Fixes several problems related to ASE service relocation and reporting in the event of network failures. • Fixes a problem that could cause the ASE daemons or asemgr utility to core dump with a segmentation violation. • Fixes a problem in which under certain circumstances, an ASE service modification could result in a corrupted configuration data base. • Fixes several TCR problems involving large sites with services containing large numbers of DRDs.

Table 3–2: Summary of TruCluster Patches (cont.)

Patch 83.00 TCR150-069	**Patch:** Fixes simple_lock timeout panic **State:** Supersedes patches TCR150-002 (1.00), TCR150-015 (31.00), TCR150-021 (19.00), TCR150-026 (24.00), TCR150-029 (26.00), TCR150-052 (64.00),TCR150-065 (76.00), TCR150-078 (90.00) This patches fixes the following problems: • Problem booting a second member into a cluster. • In a virtual hub cluster, shutting down one node can cause the other to crash. Typical panic strings on the node that crashes are: rm_failover_self and: rm_failover_all: target rail offline • Various repairs in Memory Channel error handling. Fixes for virtual hub booting with cable unplugged. • Various problems with MC errror handling discovered in cable pull under load tests. • Hubless MC2 systems hang during boot and/or experience error interrupts. • Reliable datagram (RDG) messaging support. • RDG: bug fix to the completion queue synchronization protocol. • Fixes a kernel memory fault in rm_lock_update_retry(). • Fixes a problem where both nodes in a cluster will panic at the same time with a simple_lock timeout panic.

Table 3–2: Summary of TruCluster Patches (cont.)

Patch 86.00 TCR150-074	**Patch:** Various dlm Corrections **State:** Supersedes patches TCR150-016 (14.00), TCR150-022 (20.00), TCR150-025 (23.00), TCR150-025B (37.00), TCR150-047 (50.00), TCR150-006A (5.00), TCR150-041 (66.00), TCR150-059 (71.00) This patch fixes the following problems: • Problem that can cause a cluster member to panic in rcv_deqlk_msg() with the panic string set to: dlm_panic • Provides performance enhancements that are required by Oracle V8.0.5. • Fixes a system panic with the following message: snd_grantlk_msg: no memory for message • Fixes a problem in TruCluster in which a node panics with the following string: dlm_panic • Fixes a problem in the TruCluster Production Server Software in which a system can panic with the following message: dlm getch: illegal csid • Fixes a deadlock condition between the DLM rebuild thread and the Connection Manager ping daemon (cnxpingd). The deadlock can cause users of DLM (e.g., Oracle) to hang. • Fixes a problem in which a cluster node can panic with the following panic string: convert_lock: bad lock state • Corrects a problem in which a failure in the session layer can cause DLM messages to become corrupt resulting in random DLM panic on the receiving member.

Table 3–2: Summary of TruCluster Patches (cont.)

Patch 91.00 TCR150-080A	**Patch:** TCR Available Server and Production Server Fixes **State:** Supersedes patches TCR150-003 (2.00), TCR150-009 (8.00), TCR150-011 (10.00), TCR150-017 (15.00), TCR150-018 (16.00), TCR150-020 (18.00), TCR150-023 (21.00), TCR150-024-1 (22.01), TCR150-024-2 (38.00), TCR150-033 (30.00), TCR150-037 (44.00), TCR150-051 (53.00), TCR150-032A (56.00), TCR150-005 (4.00), TCR150-038 (45.00) TCR150-043A (62.00), TCR150-048 (51.00), TCR150-056 (69.00), TCR150-049A (67.00), TCR150-061 (73.00), TCR150-060A (72.00), TCR150-062A (74.00), TCR150-063A (75.00), TCR150-064A (81.00), TCR150-068A (82.00), TCR150-071 (84.00), TCR150-073A (85.00), TCR150-075 (87.00), TCR150-076 (88.00), TCR150-077 (89.00) This patch fixes the following problems: • Fixes a problem in the message service routines used by the daemons in TruCluster Available Server and TruCluster Production Server software. When the message queue fills, the following message is entered in the daemon.log file, but the queue is not emptied: msgSvc: message queue overflow, LOST MESSAGE! From this point on, no further messages will be received. • Fixes a problem in Version 1.5 of the TruCluster Production Server and TruClusterAvailable Server products where, during the start of a service, missing special device files were not being created for HSZ disks. Since the special device files did not get created, the service start would fail. • Fixes a segmentation fault that can cause ASE daemons to exit or hang. • Fixes a problem where the Host Status Monitor (asehsm) incorrectly reports a network down (HSM_NI_STATUS DOWN) if the counters for the network interface get zeroed. • Fixes a problem that caused the asedirector to core dump if asemgr processes were modifying services from more than one node in the cluster at the same time. • Fixes scalability problems in the DECsafe Available Server, TruCluster Available Server, and TruCluster Production Server products. The problems caused the asemgr to core dump when adding or modifying services with a large number of disks. • Fixes several problems related to ASE service relocation and reporting in the event of network failures. • Fixes a problem that could cause the ASE daemons or asemgr utility to core dump with a segmentation violation. • Fixes a problem in which under certain circumstances, an ASE service modification could result in a corrupted configuration data base. • Fixes several TCR problems involving large sites with services containing large numbers of DRDs. • Fixes a problem that caused the ASE daemons and asemgr to core dump when the lookup for an IP address failed. • This is a performance improvement in the startup of start scripts. It will reduce the necessary system calls to start the scripts. • Corrects a problem in which a member add will fail in a large ASE environment.

Table 3–2: Summary of TruCluster Patches (cont.)

Patch 91.00 continued	• Corrects a problem with Networker displaying garbage characters following service names. It occurs when the service name is 8 characters or greater. • Corrects a problem which causes asemgr to core dump when modifying a drd service to add more than 200 devices in a single service. • Corrects a problem with TruCluster Available Server or Production Server cluster in which services have been started with elevated priority and scheduling algorithm. Under significant load this could lead to intermittent network and cluster problems. • Fixes a problem which caused a service not to start when there was a short network failure. This was seen only with long running stop scripts and special network configurations. • Fixes a bug where ASE picks up an extra socket after failing over. • Corrects a problem which causes an aseagent to hang when restarting the ASE member.
Patch 95.00 TCR150-080B	**Patch:** aseagent and asemgr Fixes **State:** Supersedes patches TCR150-003 (2.00), TCR150-009 (8.00), TCR150-011 (10.00), TCR150-017 (15.00), TCR150-018 (16.00), TCR150-020 (18.00), TCR150-023 (21.00), TCR150-024-1 (22.01), TCR150-024B (33.00), TCR150-024C (40.00), TCR150-032B (57.00), TCR150-043B (63.00), TCR150-049B (68.00), TCR150-060B (77.00), TCR150-062B (78.00), TCR150-063B (80.00), TCR150-064B (92.00), TCR150-068B (93.00), TCR150-073B (94.00) This patch fixes the following problems: • Fixes a problem in the message service routines used by the daemons in TruCluster Available Server and Production Server software. When the message queue fills, the following message is entered in the daemon.log file, but the queue is not emptied: msgSvc: message queue overflow, LOST MESSAGE! From this point on, no further messages will be received. • Fixes a problem in Version 1.5 of the TruCluster Production Server and Available Server products where, during the start of a service, missing special device files were not being created for HSZ disks. Since the special device files did not get created, the service start would fail. • Fixes a segmentation fault that can cause ASE daemons to exit or hang. • Fixes a problem where the Host Status Monitor (asehsm) incorrectly reports a network down (HSM_NI_STATUS DOWN) if the counters for the network interface get zeroed. • Fixes a problem that caused the asedirector to core dump if asemgr processes were modifying services from more than one node in the cluster at the same time. • Fixes scalability problems in the DECsafe Available Server, TruCluster Available Server, and TruCluster Production Server products. The problems caused the asemgr to core dump when adding or modifying services with a large number of disks. • Fixes several problems related to ASE service relocation and reporting in the event of network failures. • Fixes a problem that could cause the ASE daemons or asemgr utility to core dump with a segmentation violation.

Table 3–2: Summary of TruCluster Patches (cont.)

Patch 95.00 continued	• Corrects problems with temporary files not being removed, and eliminates the need for one temporary file. • Fixes a problem that can cause the asemgr utility to core dump when modifying services that contain a large number of disks. • Fixes a number of ASE behavior problems resulting from network cable failure. • Fixes several TCR problems involving large sites with services containing large numbers of DRDs. • Fixes a problem that caused the ASE daemons and asemgr to core dump when the lookup for an IP address failed. • This is a performance improvement in the startup of start scripts. It will reduce the necessary system calls to start the scripts. • Corrects a problem in which a member add will fail in a large ASE environment • Corrects a problem which causes asemgr to core dump when modifying a DRD service to add more than 200 devices in a single service. • Corrects a problem which causes an aseagent to hang when restarting the ASE member.