DIGITAL UNIX 4.0D and TruCluster 1.5

Patch Summary and Release Notes for Patch Kit-0008

November 2000

This manual describes the release notes and contents of Patch Kit-0008. It provides any special instructions for installing individual patches.

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

Contents

About This Manual

1 Release Notes

2 Summary of Base Operating System Patches

3 Summary of TruCluster Software Patches

Tables

About This Manual

This manual contains information specific to Patch Kit-0008 for the DIGITAL UNIX Version 4.0D 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 and TruCluster software that you are using.
- If known, the type of processor that is running the DIGITAL UNIX software.

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

1

Release Notes

This chapter provides information that you must be aware of when working with DIGITAL UNIX 4.0D and TruCluster (TCR) 1.5 Patch Kit-0008.

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 ~50.0 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 ~52.1 MB of storage space in `/var/adm/patch` may be required for original files if you choose to install and revert all patches. See *Patch Kit Installation Instructions* for more information.

  Up to ~2206 KB of storage space is required in `/var/adm/patch/doc` for patch abstract and README documentation.

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

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 ~87.1 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 ~90.0 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 ~2375 KB of storage space is required in `/var/adm/patch/doc` for patch abstract and README documentation.

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

1.2 New dupatch Features

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

1.2.1 Patch Installation from Multiuser Mode

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

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

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

1.2.2 Patch Installation from a Pseudo-Terminal

Patches can now be installed on the system from a pseudo-terminal (pty) while in single-user mode. To do this, log into the system as root from a remote location and specify that the patches are to be installed in single-user mode. Once all the patch prerequisites are completed, the system will be taken to single-user mode while maintaining the network connection for the root user. The patches will then be installed by the system.

1.2.3 Automatic Kernel Build

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

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

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

- Reboot the system immediately.
- Reboot the system at a specified time.
- Do not reboot the system.

1.3 Release Note for Patch 1005.00

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

- 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 Note for Patch 1039.00

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 non-comment 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 2 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 non-hourly command is run only once at the first occurrence
of an ambiguous clock time.

   o 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.

   o 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.

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

   o A non-hourly 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.

   o 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 Note for Patch 1089.00

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, Compaq 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.

1.6 Release Note for Patch 1045.00

In addressing a security issue, a warning message not previously seen may be placed in the `daemon.log` by `named`. An example of the message follows:

```
Jan 7 14:03:25 hostname named[316]:  owner name "xx_yy.zz.com"

IN (secondary) is invalid - proceeding anyway
```

This message has no impact on system operation and will only be seen once for any given node name on a BIND server at startup. It is informing the user that this node name contains non-standard characters. Standard characters are defined as A-Z, a-z, 0-9 and hyphen. Non-standard characters are characters that fall out of the standard set, such as underscores.

1.7 Release Note for Patch 872.00

If Patch 872.00 is installed without Patch 1035.00 (see the I/O Throttling/Smooth Sync Release Note), `unknown attribute` messages may appear, particularly upon system reboot. To remove these messages, edit the `/etc/inittab` and remove the 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
```

1.8 Release Note for Patch 1035.00

The following sections describe the release notes for Patch 1035.00.

1.8.1 I/O Throttling/Smooth Sync

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

_____ **Note** _____

Smooth Sync is for UNIX File System only.

_____

The new mount options are `smsync2` and `throttle`. The `smsync2` option 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 (the default 30 is 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 `mmap`ed pages always use this default policy, regardless of the `smsync2` setting.

For example, change the `/etc/fstab` entries from:

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

to:

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

_____ **Note:** _____

If you elect to not use `smsync2` (which does not affect `mmap`ed buffers), just remove the `smsync2` option from the previous string.

_____

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

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

When removing 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 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:

`smoothsync-age`

This variable can be adjusted 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. 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; just 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 one 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.

1.8.2 Reference Page Updates

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 above 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 non-zero 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 non-zero 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 samedisk 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 (also 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 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 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 zero, a value of 0 is returned
and the fsck command assumes that the file system does
not need to be checked.

1.8.3 Powerstorm 4D10T

This patch provides support for the Powerstorm 4D10T (ELSA Gloria Synergy)
graphics card (SN-PBXGK-BB). If you have a system with this graphics card, you
will need to reconfigure and rebuild the kernel after installing this patch. To do
this, follow these steps::

1. Shut down the system:

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

2. Boot genvmunix to single-user mode:

    >>> boot -fi genvmunix -fl s

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

    # **/sbin/bcheckrc**

    # **/sbin/update**

    # **/sbin/swapon -a**

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

    # **/usr/sbin/doconfig**

    _____ **Note:** _____

    Do not specify the –c option to doconfig. If you do, doconfig will
    use the existing kernel configuration file which will not have the
    appropriate controller entry for the Powerstorm 4D10T graphics
    card.
    _____

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

6. Shut down the system:

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

7. Boot the new kernel:

    >>> boot

If you remove this patch from your system after you have rebuilt the kernel
to incorporate support for the Powerstorm 4D10T graphics card as described
previously, you will need to rebuild the kernel again to restore generic VGA
graphics support. To do this, follow the steps given previously. The doconfig
running on the original, unpatched genvmunix will not recognize the Powerstorm
4D10T graphics card and will include generic VGA graphics support in the
resulting kernel.

1.8.4 UFS Delayed Metadata mount Option

This new mount option allows for disabling synchronous metadata writes on a
specified filesystem. The new mount option name is delayed.

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

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

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

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

To enable the `delayed` option, run:

```
mount -o delayed
```

or

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

1.9 Release Note for Patches 985.00 and 1045.00

The following sections describe the release notes for Patch 1045.00.

1.9.1 malloc(3)

`malloc` performance is enhanced for multithreaded applications.

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 below:

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 help 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.

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.

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.

1.9.2 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 non-growing.

  An arena that is non-growing 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, non-zero is returned. Otherwise, it returns zero.

RELATED INFORMATION

Functions: malloc(3)

1.10 Release Note for Patch 880.00

This is a release note for the Enhanced Round Robin Sequential Read Patch.

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 I/O 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. For 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, 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 is to attempt to hit the disk cache, and so increase performance.

The relevant tunable variables are as follows:

`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_proxmity`

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

1.11 Release Note for Patches for 726.00 and 919.00

To find more information about the ISO8859-15 functionality provided and special installation instructions related to these patches, please refer to the online README file located at:

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

From this directory, choose the link that has the following name:

`duv40dwlseco2.README`

Note

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

1.12 Release Note for Patch 1086.00

The following is an update to the `mount`(8) reference page in the AdvFS Options section of the `mount -o` Flag Options:

atimes

> Flushes to disk the file access time changes for reads
> of regular files.
> This is the default XPG4 behavior.

noatimes

> Marks file access time changes for reads of regular files
> in memory, but does not flush them to disk until other file
> modifications occur. This behavior does not comply with
> industry standards and is used to reduce disk writes for
> applications with no dependencies on file access times.

read(2):

> [DIGITAL] If the file is a regular file and belongs to an AdvFS
> fileset mounted with the AdvFS option noatimes, the read, readv,
> or pread function marks the st_atime field of the file for update.
> If the file otherwise remains unchanged, the new st_atime value
> is not flushed to disk. See mount(8) for more information on the
> noatimes mount option.

The following is an update to the *System Configuration and Tuning Guide,* Appendix B, Section 1, AdvFS Subsystem Attributes:

AdvfsPreallocAccess

    AdvFS will allocate this number of access structures to the AdvFS
    access structure freelist at startup. The minimum value is 128,
    the maximum value is 65536. The actual value allocated at startup
    will be adjusted to honor the AdvfsAccessMaxPercent configurable.

    Default value: 128

    On larger systems, a larger value than the default value of 128 may
    improve performance by slowing the rate of access structure recycling,
    allowing cached file metadata to stay in main storage.

1.13 Release Notes for Patches 911.00 and 1016.00

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

NAME

  ttauth - ToolTalk authority file utility

SYNOPSIS

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

DESCRIPTION

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

OPTIONS

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

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

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

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

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

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

COMMANDS

  The following commands may be used to manipulate authority files:

add protoname protodata netid authname authdata
> An authorization entry for the indicated ToolTalk session using
> the given protocol name (protoname), protocol data (protodata),
> ToolTalk session id (netid), authentication name (authname),
> and authentication data (authdata) is added to the
> authorization file. The protocol name should always be the
> string "TT". The protocol data should always be the empty
> string. The ToolTalk session ID is formatted string consisting
> of the ttsession program number, the ttsession authorization
> level, the IP address of the host running ttsession, and the
> RPC version number of the ttsession. See the TTSESSION
> IDENTIFIERS section below for information on constructing
> ToolTalk session ID's for the authority file. The
> authentication name should always be the string "MIT-MAGIC-
> COOKIE-1". The authentication data is specified as an even-
> lengthed string of hexadecimal digits, each pair representing
> one octet. The first digit of each pair gives the most
> significant 4 bits of the octet, and the second digit of the
> pair gives the least significant 4 bits. For example, a 32
> character hexkey would represent a 128-bit value.

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

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

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

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

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

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

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

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

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

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

TTSESSION IDENTIFIERS

The ToolTalk session identifiers (netid) in the authority file and used by
the add, [n]extract, [n]list, and remove commands are derived from the
TT_SESSION identifier constructed by ttsession at startup. The ttsession
rendezvous with clients by writing the TT_SESSION identifier as a property
on the root window or as an environment variable in the client's
environment (see ttsession -c). In addition, ttsession creates an entry in
the user's authority file. The authority file entry has a netid component
which is derived from the TT_SESSION identifier.

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

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

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

1342177279/1/130.105.9.22/4

EXAMPLE

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

% xprop -root | grep TT_SESSION

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

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

ENVIRONMENT

This ttauth program uses the following environment variables:

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

FILES

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

RESTRICTIONS

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

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

SEE ALSO

Commands: ttsession(1)

ToolTalk Reference Manual

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

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

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

1.14 Release Note for TruCluster Server

In the Production Server, Available Server, and Memory Channel environments, the TCRMAN subset is optional. However, if you choose not to install the subset during the initial installation, you will not be able to install it later.

1.15 Release Note for TCR Patch 116.00

If you are only installing TCR patches, you must rebuild the kernel and reboot the machine for the changes to take effect. If removing only TCR patches, you must also rebuild the kernel and reboot the machine for the changes to take effect.

2

Summary of Base Operating System Patches

This chapter summarizes the base operating system patches included in Patch Kit-0008.

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
Patches 1035.00, 1037.00, 1039.00, 1045.00, 1047.00, 1049.00, 1051.00, 1053.00, 1055.00, 1057.00, 1059.00, 1061.00, 1063.00, 1065.00, 1069.00, 1073.00, 1076.00, 1086.00, 1089.00, 1091.00, 1094.00, 1096.00, 1098.00, 1100.00, 1102.00, 1104.00, 1106.00, 1109.00, 1111.00, 1113.00, 1116.00, 1119.00, 1121.00, 1123.00	New

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

Patches 141.00, 33.00, 33.01, 4.00, 4.01, 27.00, 178.00, 137.00, 300.00, 307.00, 370.02, 552.00, 9.00, 10.00, 12.00, 19.00, 20.00, 18.00, 23.00, 25.00, 29.00, 30.00, 49.00, 37.00, 74.00, 39.00, 69.00, 69.01, 69.01, 91.00, 94.00, 111.00, 102.00, 119.00, 126.00, 131.00, 132.00, 83.00, 83.01, 134.00, 149.00, 107.00, 163.00, 167.00, 84.00, 145.00, 177.00, 174.01, 347.00, 180.00, 185.0, 187.00, 189.00, 190.00, 194.00, 201.00, 202.00, 206.00, 231.00, 244.00, 254.00, 255.00, 302.00, 318.00, 215.00, 356.00, 363.00, 226.00, 229.00, 238.00, 256.00, 267.00, 319.00, 354.00, 210.00, 212.00, 250.00, 251.00, 260.00, 286.00, 298.00, 272.00, 281.00, 262.00, 245.00, 266.00, 261.00, 369.00, 315.00, 313.00, 280.00, 317.00, 222.00, 295.00, 247.00, 213.00, 218.00, 191.00, 279.00, 291.00, 196.00, 304.00, 241.00, 311.00, 184.01, 220.01, 239.01, 275.01, 320.01, 277.01, 312.01, 282.00, 252.00, 253.00, 406.00, 455.00, 456.00, 457.00, 458.00, 459.00, 460.00, 461.00, 462.00, 463.00, 464.00, 465.00, 466.00, 467.00, 468.00, 469.00, 470.00, 471.00, 472.00, 473.00, 474.00, 475.00, 476.00, 477.00, 478.00, 480.00, 481.00, 483.00, 484.00, 485.00, 486.00, 487.00, 489.00, 490.00, 491.00, 493.00, 494.00, 495.00, 496.00, 497.00, 498.00, 500.00, 501.00, 345.03, 502.00, 146.00, 519.00, 559.00, 592.00, 34.00, 72.00, 72.01, 89.00, 95.00, 109.00, 237.00, 303.00, 289.02, 437.00, 438.00, 450.00, 598.00, 606.00, 612.00, 616.00, 620.00, 621.00, 547.00, 586.00, 488.00, 499.00, 640.00, 647.00, 654.00, 656.00, 665.00, 668.00, 683.00, 685.00, 687.00, 689.00, 692.00, 693.00, 695.00, 698.00, 701.00, 703.00, 712.00, 713.00, 720.00, 722.00, 725.00, 730.00, 735.00, 740.00, 746.00, 646.00, 747.00, 652.00, 697.00, 708.00, 790.00, 791.00, 792.00, 794.00, 795.00, 797.00, 800.00 802.00, 807.00, 809.00, 815.00, 816.00, 817.00, 820.00, 821.00, 823.00, 830.00, 831.00, 834.00, 836.00, 838.00, 843.00, 844.00, 849.00, 854.00, 856.00, 858.00, 860.00, 864.00, 871.00, 874.00, 875.00, 876.00, 877.00, 882.00, 884.00, 891.00, 709.00, 892.00, 803.00, 825.00, 829.00, 837.00, 842.00, 859.00, 62.00, 22.00, 40.00, 40.01, 106.00, 907.00, 710.00, 894.00, 11.01, 417.00, 426.00, 611.00, 793.00, 908.00, 926.00, 930.00, 931.00, 932.00, 933.00, 934.00, 937.00, 939.00, 940.00, 941.00, 942.00, 953.00, 959.00, 962.00, 970.00, 972.00, 976.00, 977.00, 982.00, 983.00, 984.00, 988.00, 989.00, 997.00, 1000.00, 1001.00, 1003.00, 1009.00, 1010.00, 1013.00, 965.00, 1025.00, 1026.00, 1027.00, 1028.00, 1029.00, 1030.00, 1031.00, 1032.00, 1033.00	Superseded by Patch 1035.00
Patches 45.01, 166.00, 349.02, 513.00, 531.00, 669.00, 707.00, 1011.00	Superseded by Patch 1039.00
Patches 1.00, 1.01, 110.00, 90.00, 199.00, 248.00, 258.03, 112.00, 296.02, 181.02, 78.00, 68.00, 68.01, 8.00, 8.01, 101.00, 168.00, 230.00, 6.00, 13.00, 77.01, 341.00, 360.00, 350.00, 368.00, 14.00, 75.00, 75.01, 88.00, 160.00, 162.00, 97.00, 223.00, 268.00, 273.00, 278.00, 232.00, 259.00, 362.02, 415.00, 435.00, 515.00, 528.00, 529.00, 538.00, 551.00, 555.00, 582.00, 588.00, 590.00, 614.00, 653.00, 666.00, 678.00, 686.00, 694.00, 696.00, 700.00, 705.00, 714.00, 715.00, 639.00, 639.00, 639.00, 743.00, 811.00, 901.00, 845.00, 846.00, 938.00, 850.00, 967.00, 969.00, 996.00, 1006.00, 1040.00, 1041.00, 1042.00, 1043.00	Superseded by Patch 1045.00
393.00, 396.00, 401.02, 628.00, 634.00	Superseded by Patch 1047.00
Patches 79.00, 912.00	Superseded by Patch 1049.00
Patches 172.00, 1017.00	Superseded by Patch 1051.00
Patches 987.00, 991.00	Superseded by Patch 1055.00

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

Patches 15.00, 31.00, 42.00, 42.01, 104.00, 316.02, 602.00, 676.00, 998.00	Superseded by Patch 1057.00
Patches 400.02, 540.00, 541.00, 944.00	Superseded by Patch 1063.00
Patches 153.00, 379.00, 328.00, 332.00, 333.00, 336.02, 749.00, 750.00, 751.00, 510.00, 752.00, 780.00, 914.00, 916.00, 917.00, 502.00, 334.00, 330.02, 915.00	Superseded by Patch 1065.00
Patches 155.00, 382.03, 754.00, 56.00, 171.00, 381.03, 753.00, 546.00, 756.00, 782.00, 785.00, 923.00, 1066.00 1067.00	Superseded by Patch 1069.00
Patches 155.00, 382.00, 412.02, 56.00,171.00, 381.00, 411.02, 772.00, 624.00, 775.00, 895.00, 896.00, 1021.00, 1070.00, 1071.00	Superseded by Patch 1073.00
Patches 607.00, 887.00, 851.00, 1074.00	Superseded by Patch 1076.00
Patches 82.00, 21.00, 36.00, 51.00, 41.00, 67.00, 81.00, 81.01, 93.00, 96.00, 124.00, 123.00, 115.00, 113.00, 129.00, 130.00, 133.00, 135.00, 144.00, 127.00, 138.00, 148.00, 139.00, 183.00, 188.00, 192.00, 204.00, 205.00, 209.00, 217.00, 225.00, 228.00, 235.00, 240.00, 243.00, 274.00, 285.00, 294.00, 301.00, 306.00, 308.00, 309.00, 324.00, 208.00, 284.00, 385.00, 386.00, 387.00, 388.00, 389.00, 390.00, 391.00, 392.02, 556.00, 557.00,, 558.00, 560.00, 561.00, 562.00, 563.00, 565.00, 566.00, 567.00, 568.00, 569.00, 570.00, 571.00, 573.00, 574.00, 575.00, 576.00, 577.00, 578.00, 579.00, 587.00, 629.00, 589.00, 630.00, 595.00, 596.00, 605.00, 617.00, 637.00, 638.00, 269.02, 344.00, 366.02, 660.00, 664.00, 671.00, 674.00, 675.00, 677.00, 679.00, 711.00, 721.00, 724.00, 731.00, 733.00, 738.00, 625.00, 745.00, 764.00, 765.00, 787.00, 788.00, 801.00, 806.00, 812.00, 818.00, 819.00, 833.00, 839.00, 841.00, 852.00, 865.00, 867.00, 873.00, 888.00, 767.00, 889.00, 897.00, 899.00, 900.00, 902.00, 903.00, 929.00, 935.00, 936.00, 945.00, 947.00, 950.00, 957.00, 971.00, 973.00, 980.00, 992.00, 1008.00, 927.00, 1023.00, 948.00, 1077.00, 1078.00, 1079.00, 1080.00, 1081.00, 1082.00, 1083.00, 1084.00	Superseded by Patch 1086.00
Patches 61.00, 61.01, 158.00, 398.03, 399.02, 613.00, 719.00, 729.00, 855.00, 863.00, 951.00, 958.00, 1015.00, 1087.00	Superseded by Patch 1089.00
Patches 338.01, 352.01	Superseded by Patch 1091.00
Patches 981.00, 1092.00	Superseded by Patch 1094.00
Patches 376.02, 505.00, 508.00, 553.00	Superseded by Patch 1096.00
Patches 151.00, 326.02	Superseded by Patch 1098.00
Patch 76.01	Superseded by Patch 1104.00
Patch 342.02	Superseded by Patch 1106.00
Patches 636.00, 758.00, 760.00, 1107.00	Superseded by Patch 1109.00
Patches 85.00, 351.02, 424.00, 451.00, 742.00, 862.00, 890.00, 979.00, 928.00, 1114.0	Superseded by Patch 1116.00
Patches 176.02, 425.00, 452.00, 771.00, 905.00, 906.00, 1022.00, 1117.00	Superseded by Patch 1119.00
Patch 814.00	Superseded by Patch 1123.00

Table 2–2: Summary of Base Operating System Patches

Patch IDs	Abstract
Patch 16.01 OSF425-131-1	**Patch:** System Run Level Correction **State:** Existing This patch fixes two system run level problems: • On a system running LSM, whenever there is a run level change, the lsmbstartup script runs. This causes root to be mounted read/write in single-user mode. • The bcheckrc command script continues to run even if there is an invalid root entry. This leaves the system in an unusable state in single-user mode.
Patch 32.01 OSF425-164-1	**Patch:** diskx Command Correction **State:** Existing This patch corrects the following: The /usr/field/diskx command will fail with data validation errors when specifying a block device special file for testing.
Patch 35.01 OSF425-167-1	**Patch:** Memory Leak With (dlb) Pseudodevice Driver **State:** Existing This patch fixes a memory leak problem that occurs with the STREAMS Data Link Bridge (dlb) pseudodevice driver. This problem could cause a "freeing free mbuf" panic when system memory is exhausted.
Patch 38.01 OSF425-173-1	**Patch:** vipw Issues Warnings Enhancement **State:** Existing usr/sbin/vipw now issues a warning when used to edit a large password file.
Patch 43.01 OSF425-400295-1	**Patch:** HX (PMAGB-BA) Graphic Mouse Cursor Correction **State:** Existing This patch fixes a problem with the mouse cursor when the system contains the HX (PMAGB-BA) graphics option. The cursor offset is incorrect on the Y Axis by 2 pixels.
Patch 46.01 OSF425-400406-1	**Patch:** Security, (SSRT0495U) **State:** Supersedes patch OSF425-175 (63.00) 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 54.00 OSF425DX-400012	**Patch:** Security Correction **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 64.01 OSF425-400416-1	**Patch:** who Command Correction **State:** Existing This patch fixes a problem that occurs when more than 140 users are logged on to a system and the who command is issued. If the output from the command is redirected or piped, the last several lines become corrupt.

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

Patch 66.01 OSF425-400455-1	**Patch:** Maximum Token Length Exceeded (lex) Fix **State:** Existing This patch fixes a problem with the lex command. Programs built with lex may exhibit various problems which only occur after the following warning: Maximum token length exceeded
Patch 73.01 OSF425-400465-1	**Patch:** LSM volsave Command Correction **State:** Existing This patch fixes a problem with the LSM volsave command. The volsave command returns an exit status of 1 (failure), even when the LSM configuration is successfully saved.
Patch 108.00 OSF425-208	**Patch:** make Command Correction **State:** Existing This patch fixes a problem in the make command. make checks out the file two times if there is a dependency on a file in another directory.
Patch 125.00 OSF425-228	**Patch:** AS4100, AS1200 Floppy Hang Correction **State:** Existing This patch corrects a problem on the floppy of an AS4100 with >1 GB memory, and an AS1200 with >2 DIMMs that causes the floppy operation to hang.
Patch 136.00 OSF425-245	**Patch:** Library Correction **State:** Supersedes patches OSF425-410112 (52.00), OSF425-410112-1 (52.01) This patch corrects the following: • Fixes a problem that may cause a program to cause the IEEE floating point emulator to emit this message: FATAL IEEE FLOATING POINT EMULATION ERROR • Fixes a rounding problem in the kernel software completion trap handler that slightly reduces the IEEE denormalized multiply and divide accuracy. It has no effect on typical arithmetic operations.
Patch 156.00 OSF425X11-006	**Patch:** PowerStorm 4D40T, 4D50T, or 4D60T Correction **State:** Existing This patch fixes a problem where, on systems with a PowerStorm 4D40T, 4D50T, or 4D60T graphics card, the X server may crash when running a graphics-intensive multithreaded application using a direct connection.
Patch 164.00 OSF425-405218	**Patch:** ncheck Utility on AdvFS Correction **State:** Existing This patch fixes an AdvFS problem. When running the ncheck utility with the -s option on an AdvFS file system, the command never returns but instead keeps using CPU cycles. This problem only occurs when there are no special files in the file system.
Patch 169.00 OSF425CDE-405003	**Patch:** dtbuilder Core Dump Correction **State:** Supersedes patch OSF425CDE-400010 (44.00) This patch corrects the following: • The application builder (dtbuilder) core dumps when changing the default button in the revolving property editor. • Fixes a segmentation fault in dtbuilder that occurs when a user tries to generate code using a When: Dragged From action in conjunction with the list object type.

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

Patch 175.00 OSF425-131B	**Patch:** bcheckrc Runs With Invalid Root Entry **State:** Supersedes patch OSF425-131 (16.00) This patch corrects the following: • On a system running LSM, whenever there is a run-level change, the lsmbstartup script runs. This causes root to be mounted read/write in single-user mode. • The bcheckrc command script continues to run even if there is an invalid root entry. This leaves the system in an unusable state in single-user mode.
Patch 200.02 OSF425-271-2	**Patch:** AdvFS boot Correction **State:** Existing This patch fixes a problem in which AdvFS boot code has trouble traversing symbolic links.
Patch 203.02 OSF425-274-2	**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.
Patch 211.02 OSF425-283-2	**Patch:** Environmental Monitoring (svrSystem_mib) Correction **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 227.02 OSF425-303-2	**Patch:** rmfdmn Command Correction **State:** Supersedes patch OSF425-349 (264.00) This patch corrects the following: • Fixes a problem with the rmfdmn command. The command would fail when it attempted to rename the domain to be deleted, so the domain was not deleted. However, the command returned success for the operation. • Fixes a problem with the rmfdmn command, which previously displayed success messages on the standard error device instead of the standard output device.

Patch 233.02
OSF425-310-2
	Patch: Lock Timeout/Kernel Memory Fault On 8200/8400s
	State: Supersedes patch OSF425-255 (150.00)
	This patch corrects the following:
	
	• Fixes a problem on the DIGITAL 8200/8400 machines where CPUs may be bombarded with interrupts. The high amount of interrupts may cause simple lock timeouts and kernel memory faults.
	
	• Fixes the following problems found on AlphaServer 8400/8200 class machine:
	
	  – A system hang or error messages being printed to the console. This is seen when a loadable driver is unloaded.
	
	  – A pcia error system panic or machine check.

Patch 234.02 OSF425-314-2	**Patch:** Kernel Memory Fault with faa FDDI Driver **State:** Existing This patch fixes a kernel memory fault problem that occurs with the faa FDDI driver.

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

Patch 242.02 OSF425-325-2	**Patch:** Socket Correction **State:** Existing This patch changed the sbcompress_threshold type to unsigned from signed, since you could not set the sysconfig value for this flag correctly.
Patch 246.02 OSF425-330-2	**Patch:** System Crashes **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 271.02 OSF425-356-2	**Patch:** savecore Command Correction **State:** Supersedes patch OSF425-054 (92.00) This patch corrects the following problems: • Fixes a problem with the savecore command that occurs when the primary swap device is an LSM volume. The system displays a cdcache_setup error message. • 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 than 2 GB of memory.
Patch 276.03 OSF425-361-2	**Patch:** crontab Command Correction **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.
Patch 288.02 OSF425-376-2	**Patch:** Compiler Correction **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 290.03 OSF425-380-3	**Patch:** Realtime Memory Leak Correction **State:** Existing This patch fixes the following two problems with realtime library: • A locking problem when calling sem_close() with an invalid descriptor. • A memory leak.
Patch 314.02 OSF425-412-2	**Patch:** AdvFS Command Correction **State:** Existing The vdf program is introduced as a variation of the df program that is especially suited to use with AdvFS domains and filesets.
Patch 321.02 OSF425-420-2	**Patch:** ALPHAbook 1 Panic **State:** Existing This patch fixes a problem that occurs on ALPHAbook 1 systems in which low battery status shutdown logic may cause a panic.

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

Patch 327.02 OSF425CDE-009-2	**Patch:** dtksh Command Correction **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 that 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 337.03 OSF425-405258-2	**Patch:** FDDI And Token Ring Routine Memory Leak Correction **State:** Supersedes patches OSF425-122 (5.00), OSF425-122-1 (5.01), OSF425-405186 (161.00) This patch corrects the following: • Fixes memory leaks with the FDDI and Token Ring method routines used with Extensible SNMP subagent (ESNMP). • Fixes the os_mibs source file, hrm_fs.c, which makes a call to the statfs function with 2 arguments, when statfs expects 3 arguments. • Fixes the problem where a malformed trap message sent at boot-time by the DIGITAL UNIX SNMP daemon to a Windows NT Network Management Station (NMS) could cause the NMS application or the NT operating system to crash.
Patch 340.02 OSF425-405290-2	**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 346.02 OSF425-405329-2	**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 353.02 OSF425-405360-2	**Patch:** expr Command Correction **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 355.02 OSF425-405369-2	**Patch:** rpc.lockd Correction **State:** Supersedes patch OSF425-195 (99.00) This patch corrects the following problems: • Various rpc.lockd problems. • Corrects two problems. The first change moves locked files from the message queue to the held list once. The second change adds code to allow locked files leftover from a server reboot to timeout and be transmitted to the server.
Patch 359.02 OSF425-405377-2	**Patch:** tty kernel memory fault Panic **State:** Existing This patch fixes a panic caused by freeing a pty on a reopen of the controlling tty.

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

Patch 364.02 OSF425-405406-2	**Patch:** sendmail Command Correction **State:** Existing This patch 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.
Patch 371.02 OSF425-405447-2	**Patch:** Kernel Build config Command Correction **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 372.02 OSF425-405449-2	**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).
Patch 377.02 OSF425CDE-405007-2	**Patch:** CDE File Manager (dtfile) Command Correction **State:** Existing This 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 pulldown menu.
Patch 378.03 OSF425CDE-405008-3	**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.
Patch 380.02 OSF425DX-405009-2	**Patch:** dxdiff Command Correction **State:** Existing This patch fixes a problem where dxdiff will core dump when comparing files with long lines.
Patch 394.02 OSF425-405328B-2	**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 402.02 OSF425-405279B-2	**Patch:** Networking Commands And Utilities Correction **State:** Supersedes patches OSF425-405188 (173.00), OSF425-186 (86.00), OSF425-405279 (339.00) This patch corrects the following: • Fixes hang conditions experienced with the following networking commands and utilities: rsh(1), telnet(1), ftp(1), rdate(8), ping(8), and yppush(8). • Corrects a regression problem with the rsh(1) command. • Corrects a problem with rsh(1) that is most visible with long-distance (slow) links where a packet might get dropped.
Patch 403.02 OSF425CDE-405005-2	**Patch:** dxkeyboard Application Modification **State:** Existing This patch installs a modified dxkeyboard application that correctly loads the XKB keymap for the Hebrew LK401 keyboard so that the Ctrl+Hebrew toggle key works in a DECterm window.

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

Patch 404.02 OSF425DX-410004-2	**Patch:** (svrServer_mib) Correction **State:** Supersedes patch OSF425DX-012 (329.00) This patch fixes the following problems: • Corrects unnecessary warning messages from the svrServer_mib when it could not find the thresholds.dat file. • 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
Patch 405.02 OSF425CDE-405009-2	**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 407.02 OSF425-380B-2	**Patch:** Realtime Library Correction **State:** Supersedes patch OSF425-380 (290.00) This patch fixes the following problems with realtime library: • A locking problem when calling sem_close() with an invalid descriptor. • A memory leak.
Patch 409.02 OSF425CDE-405008B-2	**Patch:** dtterm Terminal Emulator Correction **State:** Supersedes patch OSF425CDE-405008 (378.00) 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 410.02 OSF425X11-400019B-2	**Patch:** DECwindows Motif toolkit **State:** Supersedes patch OSF425X11-400019 (55.00) This patch fixes the following problem in the Bookreader library, which is part of the DECwindows Motif toolkit. When called from an application, Bookreader changes the caller's effective UID to the real UID, but then never restores it to the original effective UID, before returning control to the calling program. If an application like dxchpwd is run from a non-root account, it fails with a privilege violation.
Patch 422.00 OSF425-428A	**Patch:** libaio Shared Library Fix **State:** Existing This patch fixes applications linking the libraries libaio_raw and libpthread. Application would fail at startup with the message: Internal AIO consistency error: Cannot use libaio_raw with threads....
Patch 423.00 OSF425-428B	**Patch:** libaio Static Library Fix **State:** Existing This patch fixes applications linking the libraries libaio_raw and libpthread. Application would fail at startup with the message: Internal AIO consistency error: Cannot use libaio_raw with threads....

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

Patch 429.00 OSF425-445	**Patch:** Fix for doconfig -a And -m Options **State:** Supersedes patch OSF425-443 (427.00) This patch corrects the following: • The doconfig program incorrectly exits with a zero return code if a failure occurs. • 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 non-interactive in a situation.
Patch 433.00 OSF425-458	**Patch:** Fix For pfm Pseudo Device Driver **State:** Existing This patch prevents non-privileged users from locking up the system through incorrect use of the pfm driver.
Patch 434.00 OSF425-460	**Patch:** Fix for llogin Problem **State:** Existing This patch corrects a problem when exiting an llogin session. If the user does not enter a carriage return to display the shell prompt, the llogin will process continue to run, consuming all the free CPU time available.
Patch 436.00 OSF425-468	**Patch:** tcpslice Cmd Probs With Date Greater Than 1999 **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 441.00 OSF425-489	**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 442.00 OSF425-492	**Patch:** Fix For XTI over TCP/IP **State:** Supersedes patches OSF425-026 (2.00), OSF425-159-1 (28.01), OSF425-246-3 (182.02), OSF425-444 (428.00) This patch corrects the following: • Resolves a kernel memory fault in the xti_discon_req() routine. • Corrects a problem with the xti/streams interface module, which could result in a kernel memory fault panic during use by xti application programs. • Fixes a problem that occurs on a system when running STREAMS. The system panics with the following error message: kernel memory fault • 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 1K. When sending 4K data (using t_snd), the call is successfull but no data has been sent and no message is returned.
Patch 443.00 OSF425-495	**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 448.00 OSF425-510	**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 503.00 OSF425-520	**Patch:** Corrupt rc.config File **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.
Patch 504.00 OSF425CDE-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 506.00 OSF425CDE-405015	**Patch:** Security (SSRT0585U) **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 511.00 OSF425DX-405011	**Patch:** Fix For dxpause Program **State:** Existing This patch fixes the problem where the dxcalendar reminder displays through the pause screen (dxpause) and remains on the top of the pause window.
Patch 512.00 OSF425-405465	**Patch:** Security (SSRT0565U) **State:** Existing A potential security vulnerability has been discovered where, under certain circumstances, a terminal session may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability.
Patch 517.00 OSF425-405496	**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 518.00 OSF425-405498	**Patch:** Kernel Memory Fault Can Occur with ATMworks 351 **State:** Existing This patch fixes a kernel memory fault that can occur when running a system with a token ring adaptor and ATMworks 351.
Patch 520.00 OSF425-405504	**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 524.00 OSF425-405516	**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 525.00 OSF425-405518	**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.

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

Patch 527.00 OSF425-405524	**Patch:** gzip Cmd Has Problems Uncompressing Files **State:** Existing This patch fixes a problem in which gzip command had problem in uncompressing files larger then 4 GB.
Patch 530.00 OSF425-405540	**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 533.00 OSF425-405552	**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 534.00 OSF425-405553	**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.
Patch 535.00 OSF425-405557	**Patch:** awk -FS Cmd Displays Incorrect Output **State:** Supersedes patches OSF425-132-1 (17.01), OSF425-405482 (516.00) This patch corrects the following: • Fixes a problem in which the awk -FS command does not display the correct output. • Fixes a problem in the awk command. The maximum number of fields per record was changed from 99 to 199. • Fixes a problem with awk printing incorrectly.
Patch 536.00 OSF425-405559	**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 537.00 OSF425-405561	**Patch:** Fix for POP Mail Handler **State:** Existing This patch corrects the following: • 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 539.00 OSF425-405566	**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 544.00 OSF425X11-405014	**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.

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

Patch 548.00 OSF425-410223	**Patch:** Fix For rsh Command **State:** Supersedes patch OSF425-405507 (521.00) 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 549.00 OSF425-410225	**Patch:** voldiskadm Not Working Correctly **State:** Existing This patch corrects a LSM problem where voldiskadm was not properly handling the removal and replacement of disks that were in an error state.
Patch 550.00 OSF425-410234	**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 564.00 OSF425-456A	**Patch:** setacl Shared Library Correction **State:** Supersedes patches OSF425-405407-3 (365.03), OSF425-525A (453.00) 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. • Corrects the problem with setacl not being able to handle a user ID beginning with a numeral.
Patch 580.00 OSF425-528	**Patch:** ATM Driver May Cause System Panic **State:** Supersedes patch OSF425-269-2 (198.02) This patch corrects the following: • Provides shared-interrupt capabilities to the ATM 350 driver. • Corrects a problem in the ATM driver that could result in data inconsistency and system panic.
Patch 583.00 OSF425-532	**Patch:** Fixes For hiprof And pixie Profiling Tools **State:** Existing This patch fixes four problems whereby programs instrumented with the hiprof(5) or pixie(5) profiling tool may malfunction during execution or generate inaccurate profiles.
Patch 584.00 OSF425-533	**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 591.00 OSF425-545	**Patch:** Fix For Rewind Cmd On TZ89 Tape Drive **State:** Existing This patch fixes a problem when using the rewind command on the TZ89 tape drive. The tape subsystem returns an I/O error. It also adds support for some new devices.

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

Patch 593.00 OSF425-553A	**Patch:** Fixes Problem Recognizing terminfo Settings **State:** Supersedes patch OSF425-405453-3 (374.03) 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 a problem recognizing terminfo settings for KEY_BTAB.
Patch 594.00 OSF425-554	**Patch:** Fix for ipcs Command **State:** Supersedes patch OSF425-297-2 (221.02) This patch corrects the following: • Corrects a problem with the output format of the ipcs(1) command. • 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 600.00 OSF425-570	**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 601.00 OSF425-571A	**Patch:** libtli/libxti Shared Library Correction **State:** Supersedes patches OSF425-407-3 (310.03), OSF425-405522A (526.00) 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 604.01
OSF425-575-1
	Patch: Support for VTI Tool
	State: Supersedes patch OSF425-508 (447.00)
	This patch corrects the following:
	
	• Provides support for the Visual Threads Instrumentation (VTI) tool.
	
	• Provides the support needed for the Developer's Toolkit Update Kit.
	
	• Fixes the following problems:
	   – Segmentation fault in /sbin/loadsrv.
	   – In the License Management Facility, an incorrect amount of memory is copied, which can potentially cause data corruption.

Patch 608.00 OSF425-581	**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 618.00 OSF425-600	**Patch:** Memory Corruption Problem Caused By devz **State:** Existing This patch fixes a possible memory corruption caused by devz.

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

Patch 619.00 OSF425-641	**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. The year 2010 displays as 19110.
Patch 626.00 OSF425-456B	**Patch:** setacl Static Library Correction **State:** Supersedes patches OSF425-405407B-2 (397.02), OSF425-525B (454.00) 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 627.00 OSF425-531B	**Patch:** malloc Performance Enhancement **State:** Existing This patch fixes a problem that may cause the malloc suite of functions to show heavy mutex lock contention in multithreaded applications running on multi-CPU systems.
Patch 631.00 OSF425-553B	**Patch:** libcurses Static Library Fix **State:** Supersedes patches OSF425-405453 (374.00), OSF425-405453B-2 (408.02) 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 a problem recognizing terminfo settings for KEY_BTAB.
Patch 632.00 OSF425-571B	**Patch:** libtli/libxti Static Library Correction **State:** Supersedes patches OSF425-407B-2 (395.02), OSF425-405522B (622.00) 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 644.00 OSF425-405575B	**Patch:** Incorrect Amount Of Memory Copied In LMF **State:** Existing This patch corrects the following: • Segmentation fault in /sbin/loadsrv. • In the License Management Facility, an incorrect amount of memory is copied, which potentially can cause data corruption.
Patch 648.00 OSF425-613	**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.

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

Patch 650.00 OSF425-615	**Patch:** Fixes ATM Subsystem Problems
	State: Supersedes patches OSF425-200 (105.00), OSF425-211 (118.00), OSF425-220-1 (117.01), OSF425-452 (431.00), OSF425-484 (439.00), OSF425-499 (445.00), OSF425-487 (572.00)

This patch corrects the following:

- Fixes a problem when ATM ELANs are configured and an ATM switch reboots. This can cause a temporary connectivity problem. Hosts on Ethernet segments may not be able communicate with the DIGITAL UNIX ATM ELAN hosts until the expiration of router ARP timers.

- Fixes three ATM subsystem problems:
    - ATM UNI 3.0 will not allow UNI Version 3.1 connect setups.
    - In some cases incorrect data for the ELAN name was being used causing DIGITAL UNIX to try to join an invalid elan.
    - The utility, atmsetup(8), has been fixed to allow the elan_name option to be set in conjunction with the les option.

- Fixes the conformance problem with the DIGITAL UNIX LAN Emulation. The DIGITAL UNIX LAN Emulation client now complies with the LANE V1 spec when locating the LAN Emulation Configuration Server (LECS). The client now asks the switch via ILMI for the ATM address of the LECS.

- 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

- Adds required functional support for the FORE ATM device driver lfa.

- 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 651.00 OSF425-616	**Patch:** System Hangs Occurs When inetd Starts Daemon
	State: Existing

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 655.00 OSF425-620	**Patch:** Fix For simple_lock: time limit exceeded Panic
	State: Existing

This patch fixes a system panic with panic string:

simple_lock: time limit exceeded

Patch 657.00 OSF425-622	**Patch:** SCSI and Tape Subsystems Not Properly Evaluating Expressions
	State: Existing

This patch fixes a problem within the SCSI and tape subsystems in which an expression was not being evaluated properly.

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

Patch 658.00 OSF425-623	**Patch:** Fix For ACE EISA Driver **State:** Supersedes patch OSF425-527 (643.00) This patch corrects the following: • 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 OS with a kernel memory fault.
Patch 659.00 OSF425-624	**Patch:** System Panics With 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 662.00 OSF425-628	**Patch:** Enhancement To The ar Command **State:** Existing This patch eliminates the previous limitation on the maximum number of external symbols that could be handled by the ar command.
Patch 667.00 OSF425-635	**Patch:** Fix For newfs Command **State:** Supersedes patch OSF425-485 (440.00) This patch corrects the following: • Restores proper functionality of the /usr/bin/newfs command, which fixes several problems with that command. • 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
Patch 670.00 OSF425-639	**Patch:** syslogd Correction **State:** Supersedes patches OSF425-187 (87.00), OSF425-369-2 (283.02) This patch corrects the following problems: • Fixes a problem in which the syslogd daemon may hang when writing to a named pipe log file. • 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 673.00 OSF425-643	**Patch:** privlen And nconfig Ignored By LSM **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.

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

Patch 682.00 OSF425-652	**Patch:** Fix For NFS Problems **State:** Supersedes patch OSF425-400429-1 (70.01) This patch corrects the following: • Provides the following bug fixes and performance enhancements: – When signals causing pcnfsd to terminate or when a SIGPIPE signal was not caught, pcnfsd would exit without producing a core file. – The pcnfsd authentication would cause crashes and memory corruption. • Fixes two problems in NFS: – When starting/stopping nfs, nfs was not checking for NFS daemons running. – rpc.pcnfsd was causing core dumps when receiving a SIGTERM signal.
Patch 688.00 OSF425-660	**Patch:** Fix For stdhost Command **State:** Existing This patch fixes a problem with the stdhosts command when the file processed has lines longer than 256 characters. The error message: stdhost:malformed line "ignored" is displayed.
Patch 690.00 OSF425-663	**Patch:** Fix For I/O Hangs In ATA Driver **State:** Existing This patch corrects the following: • ATAPI IOMEGA ZIP cannot do transfers of 64 K multiples in size; it produces a SCSI parity error. • Occasional I/O hangs occur in the ATA driver.
Patch 704.00 OSF425-681	**Patch:** Fix For CDFS File System **State:** Supersedes patch OSF425-426 (418.00) This patch corrects the following: • Fixes a problem with the ddr_config command, where the -x option would intermittently fail. • 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 end of partition. Only new and non-DEC CD-ROM drives are affected.
Patch 718.00 OSF425-697	**Patch:** CDE Hangs After Logging Into System **State:** Existing This patch fixes a problem where CDE hangs after logging into a system.
Patch 726.00 OSF425-707A	**Patch:** Fix For class_admin/class_daemon Problem **State:** Existing This patch fixes a class_admin/class_daemon problem. When a PID is added to a class, it cannot be removed from the class scheduler until the process terminates or the class_scheduler has been stopped.

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

Patch 727.00 OSF425-709	**Patch:** Various Compiler Fixes **State:** Supersedes patches OSF425-155-1 (26.01), OSF425-268-2 (197.02), OSF425-457 (432.00), OSF425-568 (599.00)

This patch corrects the following:

- A run-time problem that occurred when running the SPEC 085.gcc test with the protected header files installed.

- A problem reported against the DIGITAL UNIX V4.0D C compiler for incorrect generated code for left shift of a signed int in ANSI (-std/-std1) compilation modes.

- A problem reported in comp.unix.osf.osf1 where a structure return temporary was not preserved until used in an enclosing function call.

- An internal compiler error while compiling the file events.c in the xemacs-20.3 release.

- A compiler error:

  Error: Bug found in compiler: get_expr_type: node type not known

- A problem where not enough space allocated for a function returning a structure, causing unexpected run-time results.

- A compilation error that occurred when including stdio.h and compiling in -ms (Microsoft compatibility) mode.

- A compiler crash that occurred when a mismatched #endif directive was encountered in an include file.

- A preprocessing difference that caused missing whitespace when the macro arguments included "/**/".

- A compiler error that occurred when compiling a particular type of for loop with optimization enabled.

- An optimizer error that produced incorrect results at run time when a size_t loop variable was used and the program was compiled with -O4.

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

Patch 727.00 continued	• A difference in macro processing that occurred when using wchar_t strings.
	• A compiler crash that occurred when a large parameter was passed to a routine by value.
	• A difference in preprocessor output which converted wide string literals and character constants from L" " to " ".
	• A compiler crash that occurred when a bad #pragma was encountered.
	• A compilation crash that occurred when compiling a structure containing an element of type int x[0].
	• A compiler crash that occurred when a while loop was coded using while ((pos - 1) > 0). This could be recoded as while (pos > 1).
	• An optimizer error that produced incorrect results at run time when an initialization loop was generated incorrectly if compiled -O4.
	This patch fixes the following problems in the DEC C compiler:
	• A run-time problem that caused the loss of a sign change during left shift
	• An optimizer problem that caused the reordering of an ldx_l/stx_c sequence in an asm() call.
	• A compiler problem that produced bad code at -O0, but not at the default optimization level.
	• A run-time problem that caused incorrect loop behavior with a large integer limit.
	• A run-time problem that caused incorrect output when compiled with the -O5 optimization level.
	• A run-time problem that caused incorrect output when manipulating structures in a union.
Patch 728.00 OSF425-710	**Patch:** System Hang In Audit Code May Prevent rlogins
	State: Supersedes patch OSF425-405451-2 (373.02)
	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 734.00 OSF425-716A	**Patch:** Fix For libots3 Shared Library
	State: Existing
	This patch fixes a problem in the libots3 library, which supports OpenMP parallel applications, and is caused by the failure to check the return status after certain system calls.
Patch 736.00 OSF425-718	**Patch:** su Command Core Dumps
	State: Existing
	This patch fixes a problem in which su command core dumps when calling an application using setenv and putenv.
Patch 737.00 OSF425-719	**Patch:** crashdc 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.

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

Patch 739.00 OSF425-721	**Patch:** sysconfig -q kio Cmd Returns Subsystem Error **State:** Supersedes patch OSF425-591 (615.00) 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 command sysconfig -q kio will return the following subsystem error: function not implemented
Patch 748.00 OSF425-732	**Patch:** Security (SSRT0583U, SSRT0583Z) **State:** Supersedes patches OSF425-405548 (532.00), OSF425-583 (610.00) 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 where sending mail via /usr/lib/mh/post under a Japanese locale caused part of the date to incorrectly be in Japanese.
Patch 755.00 OSF425X11-013	**Patch:** Fix For X Server System Crash **State:** Existing This patch fixes a problem where viewing certain tiff images with an image viewer crashed the X server.
Patch 761.00 OSF425CDE-017A	**Patch:** Fix For dxaccounts 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 763.00 OSF425CDE-020	**Patch:** CDE, Security (SSRT0614U) **State:** Supersedes patch OSF425CDE-405010-2 (375.02) This patch 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. These invalid entires would include remove entries that specify non-existent keys. • Repeating appointments with a frequency of daily are sometimes displayed incorrectly by the calendar manager (dtcm). Some appointments are displayed an hour earlier or an hour later than originally scheduled. • 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.

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

Patch 766.00 OSF425-672B	**Patch:** kdbx mbuf And Socket Extension Correction **State:** Supersedes patches OSF425-405244 (165.00), OSF425-695 (716.00) This patch corrects the following: • Corrects a problem with the kdbx mbuf and socket extensions. The use of these extension on some crashdumps resulted in errors and would hang. • 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. • Fixes a problem with kdbx. A core file created by kdbx was left in the root directory when recovering from a system crash.
Patch 768.00 OSF425-696B	**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.
Patch 769.00 OSF425-707B	**Patch:** Kernel Class Scheduler And libclass.a Correction **State:** Supersedes patch OSF425-204-2 (116.02) This patch corrects the following: • Fixes kernel class scheduler race condition that can leave a thread stuck without getting anymore CPU time. • libclass.a: locking semaphore modified so that if an application (class_daemon) exits while holding the semaphore, the kernel will drop it in the exit code. • 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 770.00 OSF425-716B	**Patch:** Fix For libots3 Static Library **State:** Existing This patch fixes a problem in the libots3 library, which supports OpenMP parallel applications, and is caused by the failure to check the return status after certain system calls.
Patch 773.00 OSF425CDE-017B	**Patch:** BadPixmap Error With 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 774.00 OSF425-696C	**Patch:** Fixes Table Names Generated By C++ V6.2 Compiler **State:** Supersedes patches OSF425-574B (633.00), OSF425-703 (723.00) This patch corrects the following: • 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.

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

Patch 776.00 OSF425X11-014C	**Patch:** Support For Euro Currency Using UTF-8 Unicode Locales **State:** Existing This patch provides suppport in the X11 Environment for the Euro currency symbol using the UTF-8 Unicode locales.
Patch 777.00 OSF425CDE-021	**Patch:** Security (SSRT0615U) **State:** Supersedes patch OSF425CDE-012 (554.00) 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 779.00 OSF425CDE-024	**Patch:** Fix for CDE problem with locked screen **State:** Supersedes patch OSF425CDE-405004 (170.00) This patch corrects the following: • Fixes a problem where the xset command could not clear the screen saver under CDE. • Fixes a problem where when running the Common Desktop Environment (CDE) on a system with more than one graphics card and monitor (multihead), sometimes new windows were visible when the screen was locked.
Patch 781.00 OSF425DX-034	**Patch:** checklist utility does not provide scroll bar **State:** Existing This patch fixes a problem where the checklist utility did not provide a scroll bar on higher resolution displays (1600x1200).
Patch 784.00 OSF425X11-020	**Patch:** Fix for Powerstorm 4D10T graphics board **State:** Existing 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 789.00 OSF425-692A	**Patch:** Fix for kernel memory fault with AdvFS **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 a 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 799.00 OSF425-745	**Patch:** ftpd Command Correction **State:** Supersedes patch OSF425-405395-2 (361.02) This patch corrects the following: • Fixes a problem with the ftp daemon, ftpd, and its use of authenticated user information. The daemon was using incorrect information for logging and validation of usernames. • 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 separator. With this patch, files are returned with <CR><LF> as the end-of-file separator.

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

Patch 804.00 OSF425-751	**Patch:** lex generates incorrect tables **State:** Supersedes patch OSF425-405336-2 (348.02) This patch corrects the following: • Fixes a problem in lex that causes it to not recognize the end of a comment when the final slash (/) is preceded by more than one consecutive asterisk (*). • 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 808.00 OSF425-755	**Patch:** Fix for LMF kernel memory fault **State:** Existing 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 810.00 OSF425-757	**Patch:** Fix for ris script **State:** Existing 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 813.00 OSF425-762	**Patch:** uerf command core dumps on binary errorlog files **State:** Existing This patch modifies uerf to not core on binary errorlog files with large records.
Patch 822.00 OSF425-772	**Patch:** news command fails **State:** Existing 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 824.00 OSF425-774	**Patch:** Security, (SSRT0456U) **State:** Supersedes patches OSF425-400412 (71.00), OSF425-400412-1 (71.01), OSF425-405193 (179.00) 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. • The rpc.statd process would sometimes disappear without a trace. The fix is to ignore SIGPIPEs (triggered by statd behavior). Also, this patch catches and logs other signals that would otherwise make rpc.statd disappear without a trace. • Fixes a problem where rpc.statd hangs as it tries to notify dead remote systems.
Patch 826.00 OSF425-776	**Patch:** Fix for fverify -n command **State:** Existing This patch fixes a problem of the fverify -n flag creating directores.
Patch 840.00 OSF425-794	**Patch:** Fix for mailsetup command **State:** Existing 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/<hostname>.cf: exiting

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

Patch 848.00 OSF425-803	**Patch:** ftp command causes a core dump **State:** Supersedes patches OSF425-405188 (173.00), OSF425-186 (86.00), OSF425-405279-3 (339.03), OSF425-627 (661.00) This patch corrects the following: • Fixes hang conditions experienced with the following networking commands and utilities rsh(1) telnet(1) ftp(1) rdate(8) ping(8) and yppush(8). • Corrects a regression problem with the rsh(1) command. • Corrects a problem with rsh(1) that is most visible with long-distance (slow) links where a packet might get dropped. • Fixes rsh(1) hanging forever in select(). • Fixes a coredump problem with ftp(1) when a .netrc file contains an invalid macdef (macro definition).
Patch 853.00 OSF425-809	**Patch:** Fix for volsetup script **State:** Existing This patch fixes a problem in which the volsetup script directs its error output to the wrong device.
Patch 861.00 OSF425-818	**Patch:** Various Tape Driver Corrections **State:** Supersedes patches OSF425-266 (195.00), OSF425-384-2 (293.02), OSF425-501 (446.00), OSF425–678 (702.00) This patch fixes the following problems: • Corrects a problem where the code around referencing a tape device pointer is not synchronized and a kernel memory fault results. • Implements the READ POSITION and LOCATE commands in the tape driver. Added new ioctl MTIOCRDPOS and new MTSEEK, MTSEEKDS subcommands to MTIOCTOP. • Fixes a problem with magnetic tapes. A read with a byte count smaller than the tape's blocksize returns success but sets the eei status. A subsequent failed operation sees the read eei status rather than its own. • 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. • Fixes a problem which could result in unit attention status being missed.
Patch 866.00 OSF425-824	**Patch:** Fixes unaligned access panic in dli_input **State:** Existing This patch fixes an unaligned access panic in dli_input.
Patch 869.00 OSF425-827	**Patch:** Fix for compress utility **State:** Existing 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 870.00 OSF425-829A	**Patch:** Fix for voldisksetup, voldiskadd, and newfs **State:** Existing 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 872.00 OSF425-831	**Patch:** Fix for update installation hang **State:** New This patch fixes a problem in which a hang can occur during update install.
Patch 878.00 OSF425-838	**Patch:** Fix for yppasswd command **State:** Existing 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 879.00 OSF425-840	**Patch:** Fixes libesnmp handling of duplicate registrations **State:** Existing This patch fixes libesnmp's handling of duplicate registrations.

Patch 880.00
OSF425-841
	Patch: Fixes performance problem on LSM mirrored volumes
	State: Supersedes patches OSF425-059-1 (7.01), OSF425-405412-2 (367.02), OSF425-432 (419.00)
	This patch corrects the following:
	• Fixes a problem that occurs on SMP systems using LSM in which the system panics with a "simple lock time limit exceeded" message.
	• Fixes a problem in LSM. A data corruption occurs when readv/writev coallesced via physio while in read/writeback mode.
	• Corrects the following problems:
	  – voltrace sometimes prints records out of sequence.
	  – volsetup fails to add disks to LSM because the volboot file is full.
	  – vold dumps 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.

Patch 881.00 OSF425-842	**Patch:** sysconfigdb incorrectly adds or deletes blank lines **State:** Existing This patch corrects a problem in which sysconfigdb would incorrectly add or delete blank lines to or from the target file.
Patch 883.00 OSF425-844	**Patch:** AdvFS showfdmn command may core dump **State:** Existing This patch fixes a problem in which advfs showfdmn would sometimes core dump.

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

Patch 886.00 OSF425-848	**Patch:** Security (SSRT0592U) **State:** Supersedes patches OSF425-400424-1 (65.01), OSF425-405372-2 (357.02), OSF425-814 (857.00) This patch corrects the following: • Fix for rdist utility to prevent segmentation fault. • 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; when there are many symlinks in the fileset, it can 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 898.00 OSF425-692C	**Patch:** Fix for AdvFS property list handling **State:** Existing This patch corrects two problems in AdvFS property list handling: • Creation of property list 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 904.00 OSF425-829B	**Patch:** voldisksetup incorrectly reports device errors **State:** New This patch fixes problems with the 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 909.00 OSF425CDE-026	**Patch:** Support for Catalan (ISO8859-15) **State:** Supersedes patches OSF425CDE-019 (762.00), OSF425CDE-023 (778.00) This patch corrects the following: • Provides support in the Common Desktop Environment for the Euro currency symbol using the UTF-8 Unicode locale. • 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. • Adds Catalan (ISO8859-15) to the list of languages from which users can choose when logging in. The additional item identifies the Catalan Latin-9 locale, that supports the Euro currency sign.

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

Patch 910.00 OSF425CDE-027	**Patch:** Fix for trashinfo file permissions problem **State:** Supersedes patches OSF425CDE-405023 (509.00), OSF425CDE-015 (759.00) 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. • Fixes a problem in which file permissions allow any user to write to the /.dt/Trash/.trashinfo file.
Patch 911.00 OSF425CDE-028A	**Patch:** Security (SSRT0617U) **State:** New 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 913.00 OSF425CDE-030	**Patch:** Security (SSRT0525U, SSRT0580U) **State:** Supersedes patches OSF425CDE-400015 (80.00), OSF425CDE-405021 (507.00) 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 where the Common Desktop Environment (CDE) Application Manager did not recreate the list of application groups at login. After customizing the application groups, users would see the old groups instead of the new groups.
Patch 918.00 OSF425X11-023A	**Patch:** Shared library (libDXm) fix **State:** OSF425X11-400019-3 (55.03) This patch corrects the following problems: • Fixes the following problem in the Bookreader library, part of the DECwindows Motif toolkit. When called from an application, Bookreader changes the caller's effective UID to the real UID, but then never restores it to the original effective UID, before returning control to the calling program. If an application like dxchpwd is run from a non-root account, it fails with a privilege violation. • Fixes a problem in which the svn widget of libDXm.so creates identical backgrounds and foregrounds.
Patch 919.00 OSF425X11-024	**Patch:** Provides missing compose definitions **State:** OSF425X11-022 (786.00) This patch corrects the following: • 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. • Provides missing compose definitions when in ISO8859-15 based locales for the scaron, Scaron, zcaron, and Zcaron characters.

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

Patch 921.00 OSF425X11-026	**Patch:** Fix for Turkish F keyboard problem **State:** New This patch fixes the Turkish F keyboard problem. The character Ccedilla and ccedilla characters cannot be entered directly from the keyboard.
Patch 922.00 OSF425X11-027A	**Patch:** Various X11 Server Corrections **State:** Supersedes patches OSF425X11-405012 (383.00), OSF425X11-405013-2 (384.02), OSF425X11-004 (154.00) This patch fixes the following problems: • 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. • Fixes a memory leak in the X server when processing ListExtensions() requests. • Fixes various problems with the X font server and with the X server's interaction with X font servers.
Patch 924.00 OSF425X11-029	**Patch:** X server may core dump **State:** New This patch fixes a problem where the X server could core dump or get unaligned access errors when clients used the Multi-Buffering extension.
Patch 925.00 OSF425X11-030	**Patch:** Fixes synchronization and drawing problems **State:** Supersedes patches OSF425X11-015 (757.00), OSF425X11-019 (783.00), OSF425X11-025 (920.00) This patch corrects the following: • Provides X server support for the Powerstorm 4D10T (ELSA Gloria Synergy) graphics card (SN-PBXGK-BB). • Fixes a problem where on systems with a Powerstorm 4D10T (ELSA Gloria Synergy) graphics board, sometimes the X server did not draw text correctly. • Fixes a problem where on systems with a PowerStorm 4D10T (ELSA Gloria Synergy, SN-PBXGK-BB) graphics card, sometimes lines and images aren't drawn correctly in scrolled windows. • Fixes synchronization and drawing problems in the X server for the PowerStorm 4D10T (ELSA Gloria Synergy, SN-PBXGK-BB) graphics card.
Patch 943.00 OSF425-881	**Patch:** Security (SSRT0624U) **State:** New 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 946.00 OSF425-885	**Patch:** PCI bridge-based boot device may fail to configure **State:** Supersedes patches OSF425-614 (649.00), OSF425-610 (645.00) This patch corrects the following: • 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 is unloaded. The adapter still uses the device driver code causing the system to panic with an invalid instruction fetch. • Fixes a problem with mapping a virtual address on the AlphaServer 100A and AlphaServer 2100 machines. The virtual address being mapped is truncated due to an incorrect typecast. This caused the virtual address to have an incorrect mapping. • Fixes a problem in which a PCI bridge-based boot device may fail to configure on large IO systems.

Patch 949.00
OSF425-891
	Patch: Fixes error handling in more, vi, and ex cmds
	State: Supersedes patches OSF425-316-2 (236.02), OSF425-405475 (514.00), OSF425-405510 (522.00)
	This patch corrects the following:
	
	• Fixes a problem with the vi editor environment variable EXINIT that occurs when EXINIT includes the editors so subcommand.
	
	• 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.
	
	• 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.
	
	• Fixes the error handling when invalid multibyte sequences are encountered in the more, ex and vi commands.

Patch 955.00 OSF425-900	**Patch:** Fixes a system panic when logging into the console **State:** Supersedes patch OSF425-684 (706.00) This patch corrects the following: • Fixes a problem in which system was consistently crashing by pressing keys during the transition from firmware callback to OS console handling. • Fixes a "thread_block: interrupt level call" system panic when logging into the console with real time preemption mode enabled.
Patch 956.00 OSF425-901	**Patch:** Prevents vold from dumping core **State:** New This patch prevents /sbin/vold from dumping core during an execution of a volprint or other query command.
Patch 960.00 OSF425-905	**Patch:** mdir cmd displays the date incorrectly for year 2000 **State:** New This patch fixes a problem in which the mdir command displays the date incorrectly for the year 2000.

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

Patch 961.00 OSF425-906	**Patch:** Fix For tu Driver **State:** Supersedes patches OSF425-388-2 (297.02), OSF425-562 (597.00), OSF425-651 (681.00) This patch fixes the following problems that may occur on some DE500 adapters: • The hardware setup operation may interrupt a pending ARP packet transmission. • If the cable to the adapter is not connected, the hardware setup operation will not execute. • 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 the Compaq Professional Workstation XP1000 (as well as several others in the near future). • Corrects a problem with some DE500 interfaces that use the Micro Linear ML6694F PHY.
Patch 963.00 OSF425-908	**Patch:** Non-root user cannot write to an ffm mounted file **State:** Supersedes patch OSF425-742 (796.00) This patch fixes a problem where a non-root user can no longer write to a file that is file-on-file (ffm) mounted.
Patch 966.00 OSF425-911	**Patch:** Fix for tftpd problem **State:** New This patch fixes a tftpd problem when responding to a broadcast read request. It adds the -b option to control whether to respond to any broadcasts.
Patch 968.00 OSF425-913	**Patch:** Fixes a problem with the NCR810 script **State:** New This patch fixes a problem with the NCR810 script that can cause the KZPAA/NCR810 to hang.
Patch 974.00 OSF425-919	**Patch:** Fixes a hang in the shutdown process **State:** New This patch fixes a hang in the shutdown process (shutdown now) of a system when a device has flow control switched off.

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

Patch 975.00
OSF425-920
	Patch: Fixes problems specific to AlphaServer 1200/4100
	State: Supersedes patches OSF425-350 (265.00), OSF425-355 (270.00), OSF425-348-2 (263.02), OSF425-529 (581.00), OSF425-650 (680.00), OSF425-896 (952.00)
	This patch fixes the following problems:
	
	• Fixes a problem that can cause bad pages to not be flagged during memory testing.
	
	• 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.
	
	• Fixes a problem in which correctable memory errors are being logged to the system console as well as to the binary error log.
	
	• Fixes a problem on an AS800 where DMA with memory >1 GB is done incorrectly.
	
	• Fixes a problem with pyxis systems. These systems generate extra interrupts when PCI interrupts are processed.
	
	• Fixes a problem where the memory channel fails at boot with either patch kit 4, 5, or 6 installed.
	
	• Fixes several problems specific to AlphaServer 1200 and AlphaServer 4100 systems:
	
	  – The user.log file has the following message:
	
	    redundant power supply failure
	
	  – The messages file has the following intermittent messages:
	
	    ERROR: i2c_read_temp: enviromental monitoring error
	    ERROR: i2c_read_fail_reg: enviromental monitoring error
	    ERROR: i2c_read_func_reg: environmental monitoring error
	
	  – Systems were shutting themselves down displaying the following message:
	
	    System has reached a high temperature condition.
	    Possible problem source:
	    Clogged air filter or high ambient room temperature.

Patch 978.00 OSF425-923	**Patch:** quotactl prototype now meets POSIX standards **State:** Supersedes patches OSF425-206 (103.00), OSF425-714 (732.00) This patch fixes the following problems: • Fixes a kernel memory fault in the dqget() routine. • Fixes a problem where the system can panic with a "kernel memory fault" in dqget. • Changes the quotactl prototype in /usr/include/ufs/quota.h to meet POSIX standards.

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

Patch 985.00 OSF425-931	**Patch:** Fixes dbx problems
	State: Supersedes patches OSF425-405315-2 (343.02), OSF425-383 (292.00), OSF425-254-2 (186.02), OSF425-278-3 (207.03), OSF425-449 (430.00), OSF425-405575A (542.00), OSF425-536 (585.00), OSF425-642 (672.00), OSF425-675 (699.00), OSF425-630A (663.00), OSF425-654A (684.00), OSF425-826 (868.00)

This patch corrects the following:

- Fixes an AdvFS problem that occurs when the rmvol command is stopped before the commmand successfully removes a volume from a domain. As a result, the showfdmn and addvol commands interpreted the volume as still in the domain (although with no data available) and a balance operation returned the following AdvFS error message:

  get vol params error EBAD_VDI (-1030)

- Fixes three /usr/sbin/lmf date problems:

  – LMF improperly handles 2-digit dates between 2000 and 2068.

  – When LMF is given two consecutive 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.

- Segmentation fault in /sbin/loadsrv.

- In the License Management Facility, an incorrect amount of memory is copied, which potentially can cause data corruption.

- This patch is required for users who wish to view user stacktraces from full crash dumps with dbx.

- Corrects a problem where the /sbin/kloadsrv process may hang and not respond to /usr/sbin/netstat commands. When this occurred, the error reported by netstat was no namelist.

- Fixes a problem in viewing a variable subrange parameter from a Pascal module while using dbx.

- 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

- Corrects some error messages given when the AdvFS utility verify(8) detects file errors. It also corrects a problem whereby verify was unable to delete files with no directory entries.

- Fixes a problem with multi-volume 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.

- Fixes three problems in dbx:

  – Most instances of incomplete stack tracing now show the whole stack.

  – Assignment to a variable would fail after viewing a non-local symbol.

  – The use of vfork would raise a signal 66.

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

Patch 986.00 OSF425-932	**Patch:** Change to error messages
	State: Supersedes patches OSF425-405374-2 (358.02), OSF425-405580 (543.00)

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.

- Prevents the message "nfscast: select: Invalid argument" message from appearing in the daemon.log when the server is not available. It also changes the "trymany: servers not responding: RPC: Unable to receive" message to an informational rather than an error message.

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

Patch 990.00 OSF425-936	**Patch:** Fix for linker problem **State:** Supersedes patches OSF425-218 (120.00), OSF425-263 (193.00), OSF425-043-1 (58.01), OSF425-291 (216.00), OSF425-342 (257.00), OSF425-217 (121.00), OSF425-434-2 (323.02), OSF425-439 (421.00), OSF425-574A (603.00), OSF425-724 (741.00), OSF425-042-1 (57.01), OSF425-696A (717.00), OSF425-785 (832.00)

This patch corrects the following:

- Addresses two issues with the /sbin/loader:

  – Fixes an infinite loop in /sbin/loader.

  – Changes the /sbin/loader so that it now reports the names of unresolved symbols in a shared library which is opened by a dlopen() call.

- Fixes a problem where the linker might crash when printing out lengthy error diagnostics.

- Fix for a linker problem that could cause incorrect symbol resolution in call_shared applications. The result is the application may use a shared library's version of a symbol rather than a symbol with the same name defined in the application.

- Fixes a problem that occurs when the default C compiler is used to compile a program using the following switches on the command line:

  -c -compress -fast

- Implements a new cc switch to allow the passing of the ld -input file switch to the linker via cc, without changing its relative position in the ld command line. The current method for doing this (-Wl,-input,filename) changes the order in which such a file is presented to the linker, and can result in an invalid transfer address in an executable, resulting in a segmentation fault.

- Fixes a problem in cc that causes it to set the incorrect optimization level when the user specifies the -O -migrate options.

- 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 latent support for DCPI, a performance analysis tool.

- 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 segfaults in nm for object files generated by the C++ compiler.

- 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.

- Fixes a linker problem where including a shared library on a link line twice with another library in between caused unresolved symbols in some cases.

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

Patch 993.00 OSF425-939A	**Patch:** Adds missing prototype for the stime function
	State: New
	This patch adds the missing prototype for the stime() function to <sys/time.h>, allowing C++ programs and other software to properly resolve it.

Patch 994.00 OSF425-940	**Patch:** find Command Correction
	State: Supersedes patch OSF425-295-2 (219.02)
	This patch corrects the following problems:
	• Fixes the find command in which files in directories which were mounted with the -fstype nfsv2 argument were not found.
	• Fixes a problem with the find command. Find fails to show filenames that start with a period.

Patch 995.00 OSF425-941	**Patch:** Fix for restore command problem
	State: Supersedes patches OSF425-333-2 (249.02), OSF425-512 (449.00)
	This patch fixes the following problems:
	• 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.
	• Fixes a problem in which the restore command can fail with the following error:
	Cannot malloc space for property list

Patch 999.00 OSF425-947	**Patch:** Danish locale now uses all lowercase month names
	State: Existing
	This patch updates the Danish (da_DK.ISO8859-1) locale to use all lowercase month names.

Patch 1002.00 OSF425-950	**Patch:** Problem occurs when sorting multibyte locales
	State: Supersedes patches OSF425-405154 (157.00), OSF425-405514 (523.00), OSF425-847 (885.00)
	This patch corrects the following:
	• Fixes the error condition that the sort command may erroneously skip 8-bit characters when the -d or -i option is specified.
	• 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.
	• Fixes a problem that sometimes occurs when sorting large data files in a multibyte locales like Japanese.

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

Patch 1004.00 OSF425-952	**Patch:** psiop driver fails when vdump is used **State:** Supersedes patches OSF425-375-2 (287.02), OSF425-744 (798.00) This patch corrects the following: • 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) • Fixes a problem with the psiop driver that causes it to fail when vdump is used. The following error is displayed: vdump : unable to write to device
Patch 1005.00 OSF425-953	**Patch:** btcreate does not wait long enough between vdumps **State:** Supersedes patches OSF425-391-2 (299.02), OSF425-752 (805.00), OSF425-802 (847.00), OSF425-855 (893.00), OSF425-909 (964.00) This patch corrects the following: • Fixes a scanset processing problem in swscanf(). • Corrects a problem in the btextract script that 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 with the btcreate command where it does not pass the full pathname to newfs. • Fixes a problem with the btcreate command where default restore fails if disklabel is different. • Fixes a problem with btcreate not waiting long enough for the next tape to be loaded with some media changers.
Patch 1007.00 OSF425-955	**Patch:** Problem with Memory Channel driver panics **State:** Supersedes patches OSF425-400 (305.00), OSF425-421-2 (322.02) This patch fixes the following problems: • Fixes a problem that can cause a panic with the message: rm_failover_self This panic occurs in a virtual hub environment when the member with VH1 is powered off. This patch also contains general fixes for handling Memory Channel errors. • Adds support for the Memory Channel 2 controller in the TCR environment. • Fixes a problem in the Memory Channel driver which could result in panics with rm-inconsistent local spinlock structures being logged.
Patch 1012.00 OSF425-961	**Patch:** Cursor displayed incorrectly **State:** New This patch fixes a problem where the cursor is displayed incorrectly when the image plane is set to 1 and the mask plane is set to 0.

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

Patch 1014.00 OSF425-969	**Patch:** Panic when running Classical IP over lfa ATM driver **State:** Supersedes patches OSF425-191 (140.00), OSF425-199 (100.00), OSF425-201 (128.00), OSF425-288-2 (214.02), OSF425-496 (444.00) This patch corrects the following: • Fixes a problem in which an ATM CLIP connection does not send data. • Fixes a kernel memory fault in atmip_proc_esi. • Fixes a problem that occurs on a system running ATM. The system panics with a "kernel memory fault" due to a simple lock time violation. Prior to the crash, the pvc flag is observed as stale on a permanent virtual circuit. The crash occurs after the pvc is deleted with the following command: # atmconfig -pvc ..... • Fixes an interoperability problem with CISCO CLIP clients. • Fixes a problem in which systems that use the Compaq Tru64 UNIX ATM CLIP interface may run out of memory. • Fixes a kernel panic seen when running Classical IP over the lfa ATM driver. This panic would only occur in lockmode 4. If not in lockmode 4, the symptom would be a CPU hang.
Patch 1016.00 OSF425CDE-028B	**Patch:** Security (SSRT0617U) **State:** New 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 1018.00 OSF425X11-023B	**Patch:** Static library (libDXm) fix **State:** New This patch fixes a problem in which the svn widget of libDXm.so creates identical backgrounds and foregrounds.
Patch 1020.00 OSF425X11-027B	**Patch:** Fix for X server interaction with X font server **State:** Supersedes patch OSF425X11-405015 (545.00) This patch corrects the following: • Fixes a problem where the X font server (xfs) sometimes failed with a segmentation fault when it received an invalid request. • Fixes various problems with the X font server and with the X server's interaction with X font servers.
Patch 1024.00 OSF425-939B	**Patch:** C++ programs can now resolve stime function **State:** New This patch adds the missing prototype for the stime() function to <sys/time.h>, allowing C++ programs and other software to properly resolve it.

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

Patch 1035.00	**Patch:** Security (SSRT0521U, SSRT0537U)
OSF425-1007	**State:** New. Supersedes patches OSF425-189 (141.00), OSF425-165 (33.00), OSF425-165-1 (33.01), OSF425-091 (4.00), OSF425-091-1 (4.01), OSF425-156 (27.00), OSF425-405202 (178.00), OSF425-222 (137.00), OSF425-392 (300.00), OSF425-403 (307.00), OSF425-405432-2 (370.02), OSF425-410246 (552.00), OSF425-064 (9.00), OSF425-066 (10.00), OSF425-080 (12.00), OSF425-120 (19.00), OSF425-121 (20.00), OSF425-146 (18.00), OSF425-148 (23.00), OSF425-153 (25.00), OSF425-160 (29.00), OSF425-161 (30.00), OSF425-405120 (49.00), OSF425-170 (37.00), OSF425-400461 (74.00), OSF425-178 (39.00), OSF425-400451 (69.00), OSF425-400451-1 (69.01), OSF425-400451-1 (69.01), OSF425-188 (91.00), OSF425-192 (94.00), OSF425-196 (111.00), OSF425-213 (102.00), OSF425-223 (119.00), OSF425-229 (126.00), OSF425-231 (131.00), OSF425-236 (132.00), OSF425-061A (83.00), OSF425-061A-1 (83.01), OSF425-242 (134.00), OSF425-248 (149.00), OSF425-202 (107.00), OSF425-405207 (163.00), OSF425-405238 (167.00), OSF425-172 (84.00), OSF425-252 (145.00), OSF425-176 (177.00), OSF425-284-1 (174.01), OSF425-405330 (347.00), OSF425-230 (180.00), OSF425-253 (185.00), OSF425-256 (187.00), OSF425-258 (189.00), OSF425-260 (190.00), OSF425-265 (194.00), OSF425-272 (201.00), OSF425-273 (202.00), OSF425-277 (206.00), OSF425-308 (231.00), OSF425-328 (244.00), OSF425-339 (254.00), OSF425-340 (255.00), OSF425-396 (302.00), OSF425-416 (318.00), OSF425-289 (215.00), OSF425-405371 (356.00), OSF425-405404 (363.00), OSF425-302 (226.00), OSF425-306 (229.00), OSF425-319 (238.00), OSF425-341 (256.00), OSF425-352 (267.00), OSF425-417 (319.00), OSF425-405362 (354.00), OSF425-282 (210.00), OSF425-285 (212.00), OSF425-334 (250.00), OSF425-335 (251.00), OSF425-345 (260.00), OSF425-372 (286.00), OSF425-389 (298.00), OSF425-357 (272.00), OSF425-367 (281.00), OSF425-347 (262.00), OSF425-329 (245.00), OSF425-351 (266.00), OSF425-346 (261.00), OSF425-405426 (369.00), OSF425-413 (315.00), OSF425-411 (313.00), OSF425-365 (280.00), OSF425-415 (317.00), OSF425-298 (222.00), OSF425-386 (295.00), OSF425-331 (247.00), OSF425-287 (213.00), OSF425-293 (218.00), OSF425-261 (191.00), OSF425-364 (279.00), OSF425-381 (291.00), OSF425-267 (196.00), OSF425-398 (304.00), OSF425-324 (241.00), OSF425-408 (311.00), OSF425-249-1 (184.01), OSF425-296-1 (220.01), OSF425-320-1 (239.01), OSF425-360-1 (275.01), OSF425-418-1 (320.01), OSF425-362-1 (277.01), OSF425-410-1 (312.01), OSF425-368 (282.00), OSF425-336 (252.00), OSF425-337 (253.00), OSF425-379 (406.00), OSF425-405459 (455.00), OSF425-405491 (456.00), OSF425-405579 (457.00), OSF425-405590 (458.00), OSF425-409 (459.00), OSF425-424 (460.00), OSF425-425 (461.00), OSF425-441 (462.00), OSF425-448 (463.00), OSF425-455 (464.00), OSF425-463 (465.00), OSF425-465 (466.00), OSF425-467 (467.00), OSF425-469 (468.00), OSF425-475 (469.00), OSF425-476 (470.00), OSF425-486 (471.00), OSF425-488 (472.00), OSF425-490 (473.00), OSF425-491 (474.00), OSF425-494 (475.00), OSF425-497 (476.00), OSF425-505 (477.00), OSF425-506 (478.00), OSF425-518 (480.00), OSF425-521 (481.00), OSF425-541 (483.00), OSF425-546 (484.00), OSF425-549 (485.00), OSF425-551 (486.00), OSF425-552 (487.00), OSF425-557 (489.00), OSF425-558 (490.00), OSF425-560 (491.00), OSF425-565 (493.00), OSF425-567 (494.00), OSF425-569 (495.00), OSF425-577 (496.00), OSF425-578 (497.00), OSF425-585 (498.00), OSF425-594 (500.00), OSF425-595 (501.00), OSF425-405328-3 (345.03), OSF425-601 (502.00), OSF425-240 (146.00), OSF425-405500 (519.00), OSF425-447A (559.00), OSF425-547A (592.00), OSF425-166 (34.00), OSF425-400458 (72.00), OSF425-400458-1 (72.01), OSF425-185 (89.00), OSF425-198 (95.00), OSF425-216 (109.00), OSF425-318 (237.00), OSF425-397 (303.00), OSF425-378-2 (289.02), OSF425-474 (437.00), OSF425-477 (438.00), OSF425-522 (450.00), OSF425-563 (598.00), OSF425-579 (606.00),

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

Patch 1035.00 continued	OSF425-588 (612.00), OSF425-592 (616.00), OSF425-517 (620.00), OSF425-582A (621.00), OSF425-410219 (547.00), OSF425-537A (586.00), OSF425-556 (488.00), OSF425-586A (499.00), OSF425-667 (640.00) OSF425-612 (647.00), OSF425-619 (654.00), OSF425-621 (656.00), OSF425-633 (665.00), OSF425-636 (668.00), OSF425-653 (683.00), OSF425-656 (685.00), OSF425-658 (687.00), OSF425-661 (689.00), OSF425-665 (692.00), OSF425-666 (693.00), OSF425-670 (695.00), OSF425-673 (698.00), OSF425-677 (701.00), OSF425-679 (703.00), OSF425-690 (712.00), OSF425-691 (713.00), OSF425-699 (720.00), OSF425-702 (722.00), OSF425-706 (725.00), OSF425-712 (730.00), OSF425-717 (735.00), OSF425-723 (740.00), OSF425-730 (746.00), OSF425-611 (646.00), OSF425-731 (747.00), OSF425-617 (652.00), OSF425-672A (697.00), OSF425-686A (708.00), OSF425-734 (790.00), OSF425-736 (791.00), OSF425-738 (792.00), OSF425-740 (794.00), OSF425-741 (795.00), OSF425-743 (797.00), OSF425-746 (800.00), OSF425-749 (802.00), OSF425-754 (807.00), OSF425-756 (809.00), OSF425-764 (815.00), OSF425-765 (816.00), OSF425-766 (817.00), OSF425-770 (820.00), OSF425-771 (821.00), OSF425-773 (823.00), OSF425-781 (830.00), OSF425-784 (831.00), OSF425-787 (834.00), OSF425-790 (836.00), OSF425-792 (838.00), OSF425-798 (843.00), OSF425-799 (844.00), OSF425-804 (849.00), OSF425-810 (854.00), OSF425-812 (856.00), OSF425-815 (858.00), OSF425-817 (860.00), OSF425-822 (864.00), OSF425-830 (871.00), OSF425-833 (874.00), OSF425-834 (875.00), OSF425-836 (876.00), OSF425-837 (877.00), OSF425-843 (882.00), OSF425-845 (884.00), OSF425-853 (891.00), OSF425-687 (709.00), OSF425-854 (892.00), OSF425-750A (803.00), OSF425-775A (825.00), OSF425-780A (829.00), OSF425-791 (837.00), OSF425-797A (842.00), OSF425-816A (859.00), OSF425-145 (62.00), OSF425-149 (22.00), OSF425-179 (40.00), OSF425-179-1 (40.01), OSF425-212 (106.00), OSF425-862 (907.00), OSF425-688 (710.00), OSF425-856 (894.00), OSF425-068-1 (11.01), OSF425-394 (417.00), OSF425-442 (426.00), OSF425-584 (611.00), OSF425-739 (793.00) OSF425-872 (908.00) OSF425-846 (926.00), OSF425-861 (930.00), OSF425-865 (931.00), OSF425-866 (932.00), OSF425-867 (933.00), OSF425-868 (934.00), OSF425-873 (937.00), OSF425-875 (939.00), OSF425-876 (940.00), OSF425-877 (941.00), OSF425-878 (942.00), OSF425-898 (953.00), OSF425-904 (959.00), OSF425-907 (962.00), OSF425-915 (970.00), OSF425-917 (972.00), OSF425-921 (976.00), OSF425-922 (977.00), OSF425-928 (982.00), OSF425-929 (983.00), OSF425-930 (984.00), OSF425-934 (988.00), OSF425-935 (989.00), OSF425-944 (997.00), OSF425-948 (1000.00), OSF425-949 (1001.00), OSF425-951 (1003.00), OSF425-957 (1009.00), OSF425-958 (1010.00), OSF425-962 (1013.00), OSF425-910A (965.00), OSF425-996 (1025.00), OSF425-1025 (1026.00), OSF425-979A (1027.00), OSF425-965 (1028.00), OSF425-988 (1029.00), OSF425-967 (1030.00), OSF425-978 (1031.00), OSF425-997 (1032.00), OSF425-1019 (1033.00) This patch corrects the following: • Allows kernel patching to fix a situation when printing using LAT to slow printers; the end of a large file fails to print, yet no error is reported. • Fixes a problem in the streams code which could have resulted in data corruption. • The ASDU netbeui server (nbelink) will not close a connection. It will hang in dlcb_close awaiting a STREAMS event. Subsequently, new connections will not be able to connect to nbelink.

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

Patch 1035.00 continued	• Applications running System V pseudoterminal slave pty can hang forever on open() system call.
	• Fixes a problem that occurs on a system when running STREAMS. The system panics with the following error message:
	kernel memory fault
	• 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 error message "kernel memory fault".
	• Fixes a problem in which the system panics with one of the following error messages:
	simple_lock: uninitialized lock
	simple_lock_terminate: lock busy
	• 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 problem in mountd where lines in the /etc/exports file could be no longer than 1023 characters. With this patch, a trailing backslash character in the /etc/exports file allows continuations beyond 1023 characters.
	• 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 with the mount command where it sometimes kills other processes.
	• Fixes a problem in AdvFS that could cause thread hangs or a system panic.
	• Provides a fix to avoid a panic that might result when running a mixed filesystem behind the HSZ70 RAID controller on the KZPSA-BB Fast10 Wide Differential Adapter in cluster environments under DIGITAL UNIX V4.0D, in conjunction with Version A11 (or greater) KZPSA firmware.
	• Fixes a problem that occurs on AlphaServer 4100 systems. If no devices are attached to the KZPSA disk controller, the system may panic when attempting to perform I/O.
	• Provides a set of workarounds for Qlogic firmware bugs. These bugs were encountered when using the HSZ70 RAID Array Controller on the KZPBA-CB wide differential UltraSCSI Adapter in a dual-node cluster environment.
	• Fixes a panic with the following error message:
	trap: invalid memory write access from kernel mode
	• Fixes a problem that occurs when KZPSA and KZTSA hardware resources needed to do I/O are unavailable causing a large number of events to be logged. The system can become sluggish and sometimes crash. This problem is seen on 8400 and 4100 systems with limited hardware scatter-gather memory resources.

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

Patch 1035.00 continued	• Fixes a problem in which a failed KZPSA adapter panics the kernel. It also fixes a problem in which CAM status was returning an incorrect NO HBA status for miscellaneous SIMPORT errors, instead of the correct CAM BUSY status.
	• Corrects a problem that can result in a kernel memory fault during heavy SCSI I/O, particularly on a small-memory system.
	• 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 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 listed below:
	panic ("(spo_process_rsp) ran out of memory!")
	• Fixes a panic which has the following error message:
	lw_remove: light weight wiring(s) found
	• Fixes a kmf problem when the type of SCSI device dynamically changes.
	• Fixes a panic when booting with TCR 1.5 software. When the system tries to initialize the ASE Availability Manager during boot, it gets a kernel memory fault.
	• Provides the DEGPA-SA Gigabit Ethernet driver support.
	• Fixes a problem where process accounting data is not written to the accounting file when it is on an NFS-mounted file system. This problem occurs on Dataless Management Services (DMS) client systems.
	• Fixes a problem in mountd where multiple A records in DNS database for an NFS client will not always succeed.
	• Fixes a panic with the following panic string:
	pgmv: session leader attempted setpgrp
	• 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 which employ SCS threads of different priorities.
	• 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 routine spec_reclaim.
	– When executing the file command against a lat (BSD) special device, the file process will hang.
	– On multi-CPU systems, hangs can occur in the revoke system call when multiple threads attempt to call revoke at the same time.

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

Patch 1035.00 continued	• Fixes a kernel memory fault caused by a streams SMP race condition.
	• Fixes a problem where several processes accessing the same AdvFS file can hang in ubc_lookup().
	• Provides support for the DAPCA HE622 and the DAPBA HE155 ATM adapters.
	• Fixes a kernel memory fault and an SMP race condition with the AltaVista Firewall 98 server on a multi-CPU system.
	• 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 system hang in which there is a large number of pending IOCTLs on the streams queue.
	• Fixes a problem on systems running screend where TCP/IP fragments are being dropped.
	• This patch fixes two problems:
	– Callback thread blocking forever in isp_enable_lun
	– assert wait in xpt_ccb_alloc panic
	• 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 DLPI. It is not possible to configure DLPIs maximum link parameters. Therefore, max_links and max_macs parameters have been made configurable using sysconfig.
	• 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 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 which the fsck utility may be unable to repair a UFS filesystem.
	• Fixes a problem in which the system may panic with the following error message:
	kernel memory fault
	• Fixes a panic in the kernel. The panic has the following error message:
	simple_lock: time limit exceeded

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

Patch 1035.00 continued	• Fixes a system pause seen when doing a lot of I/O to UFS filesystems.
	• Improves UFS performance by no longer prematurely writing single pages.
	• Fixes system crashes seen on ASE or TruCluster 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.
	• This patch fixes and enhances the quotacheck and fsck commands.
	• Fixes a problem in which mount would incorrectly fall back to Version 2 after certain errors had been encountered using Version 3.
	• Fixes an nfs/ufs/vm deadlock. While serving a client, the system running ASE/DT as an NFS server can hang with deadlock.
	• Removes the following message, seen when booting with genvmunix on large-memory systems:
	contig_malloc: failed to allocate memory within addrlimit
	• Fixes two problems:
	– Fork can fail to obtain swap space.
	– Resource limitation on core files does not work as documented.
	• Provides the driver and related kernel support for the Powerstorm 4D10T (ELSA Gloria Synergy) graphics card (SN-PBXGK-BB).
	• 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 string "simple_lock_terminate: lock busy".
	– A system panic, with panic 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.
	• Ensures all AdvFS root fileset buffers are flushed on shutdown.
	• Fixes a UFS file system panic with the following error message:
	malloc_check_checksum: memory pool corruption

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

Patch 1035.00 continued	• Fixes the database application core dumps when using truss/trace tools by remembering that COW has been set up on a shared pte and processes it correctly when a subsequent write access is made to the page.
	• Fixes a problem with NFS locking when lockmode is set to 4. The system can panic with "lock_write: hierarchy violation" or "lock_write: simple lock owned".
	• Fixes a problem in which the system may memory fault if the TCR/ASE server no longer has access to the CD-ROM device.
	• Forces the kernel malloc code to print failure messages only when kmem_debug is enabled and also corrects some other minor kmem_debug problems.
	• Fixes a class scheduler problem seen when scheduling PIDs. The PID class scheduling heuristics have been changed so that a child does not inherit its parent's class scheduling policy.
	• 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 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 data corruption problem that can occur when mapping to private regions.
	• Fixes a problem in which signals can be lost in multithreaded applications.
	• Improves NFS performance by avoiding an undesired cache invalidation that can have a big impact on NFS performance with huge files.
	• Fixes a problem where RCP commands issued from a Sun Solaris system to DIGITAL UNIX may sometimes fail incorrectly with the error message:
	Connection reset by peer
	• Fixes a simple_lock: hierarchy violation in sigq_abort() when lockmode is set to 4.

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

Patch 1035.00 coninued	• Fixes a problem that causes CPU0 in a multi-CPU system to hang in the socket close routines.
	• Fixes a kernel memory fault caused when a network application walked an inpq array.
	• Fixes system crashes seen on ASE or TruCluster systems when changing the network interfaces. The stack is not informative and the panic may be "trap: illegal instruction," or "kernel memory fault."
	• Fixes two problems:
	– Locking/unlocking of a segmented shared memory region causes the system to panic with the following message:
	(cpu 0): vm_page_ssm_unwire
	– The segmented shared memory does not handle simultaneous shared memory locks and unlocks, causing the system to panic with the following message:
	ssm_anon_free: wired/held/busy page
	• Fixes a problem with soclose() that caused permanent looping on exit while aborting pending connections at a TCP/IP listener socket.
	• Fixes a problem that only occurs if realtime pre-emption is enabled and SMP test suites are run.
	• 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 with virtual memory. When running the Oracle database, the Oracle software cannot detach from a shared memory segment.
	• Fixes single-step support in a debugger, such as Ladebug, for instructions that trap or fault.
	• Fixes an incorrect calculation for memory-usage-by-type when kmem_debug is set.
	• Corrects a problem in which the wrong status could be returned when using a tape device.
	• Fixes a problem where all nodes in a cluster can panic at the same time with a simple_lock timeout panic.

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

Patch 1035.00 continued	• 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 either a performance degradation, command timeouts, or in the worst cases a system hang condition.
	• Fixes a TCP performance problem if the TCP window scale option is turned off when using the HIPPI interface.
	• Fixes a problem where a possible unaligned access fault can occur in the kernel.
	• Fixes a problem with tmv2_notify_cbf messages being logged from KPBSA adapters and creating very large binary.errlog files in a clustered environment.
	• Fixes a problem in which the system can panic with a kernel memory fault.
	• Upgrade to the Gigabit Ethernet driver Version 1.0.12 to fix various performance problems.
	• Fixes a problem where the system can panic with the panic string "secsize_resid < d_reclen" when accessing a defective CD-ROM.
	• Fixes a system hang condition. All NFS-related services may deadlock.
	• Fixes a problem where partitioned Turbolasers return incorrect CPU data for CPUs that are not in the partition.
	• Fixes a problem on systems with a Powerstorm 4D10T (ELSA Gloria Synergy) graphics board, where the graphics were not reset to console mode (the blue screen) when the halt button was pressed.
	• Fixes a problem where ubc_msync() may not flush out all the pages in requested range.
	• Fixes callback on freed CCB panics.

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

Patch 1035.00 continued	• Provides changes necessary for AV firewall 98 to pass ICSA certification.
	• Fixes var adm messages from truncation on larger configurations by raising the default size (4096) of msgbuf_size to 8192.
	• Fixes a problem with the parameter-checking code of the fcntl system call. As a result, incorrectly coded fcntl() parameters in user programs no longer panic the system.
	• Fixes the AdvFS race between extending and reading subextent maps and avoids the panic in advfs bs_get_bf_xtnt_map code (QAR 61985). This patch also fixes the race with removing storage causing kernel memory fault (QAR 66890).
	• 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 could result in a incorrect scheduling of threads when they were dispatched from the idle state.
	• 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 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 problem where systems with the DUV40DAS0005-19991007 patch kit installed would run low on kernel memory after process accounting had been running for a while.
	• Fixes a problem in a cluster configuration with the fta FDDI driver. The console message seen for this problem is:
	hw_sg_load: load request too big, pages alloced 1 required 2
	• Fixes a kernel memory fault caused by the fta FDDI driver.
	• Fixes a problem that may occur on systems with an FDDI controller. During system boot, the system may panic with a message similar to the following:
	panic (cpu 8): kernel memory fault
	• Corrects a problem with the FDDI fta driver.
	• Fixes a kernel memory fault caused by a mishandling of multicast addresses on the FDDI interface.
	• Fixes a problem with virtual mac addressing.

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

Patch 1035.00 continued	• Fixes a problem in which a system may crash if multiple bad blocks on a SCSI device are encountered simultaneously.
	• 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 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-IO basis, and the times did not account for overlapping I/O.
	• Fixes the problem that causes a ccmn_rem_ccb3 panic not on any list and a device starvation problem when Rapid Error Recovery is in use.
	• Fix to prevent I/O stalling infinitely when ccb queue on a device is full.
	• 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 .
	– Fixes simple_lock timeouts holding the ubc_lru_lock too long.Fixes a problem where programs that read, analyze and monitor disk statistics (such as "collect") will occasionally display incorrect results.
	– Fixes a problem in which the interaction between mfs file systems and smoothsync causes procprod to read stale data.
	– Fixes a problem in which the system can panic with a kernel memory fault during an installation with an HSZ70 or HSZ80 connected to the system.
	– Fixes a kernel memory fault when accessing the vm_map_index hash table.
	– Fixes a simple_lock time limit exceeded panic due to an SMP race condition in namecache.
	– Fixes a problem that causes corruption in the floating point registers whereby the flag fields nxm_fp_owned are overwritten with 0s.
	– Fixes a kernel memory fault in VMAC code if_addnewaddr().
	– Fixes a kernel memory fault in procfs_get_s5_dir.
	– Fixes a system panic with panic string:
	psig: catch not set
	– Corrects a kernel memory fault caused by rw3vp_cache passing a bad address to _OtsZero().

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

Patch 1035.00 continued	• Fixes a problem in which an application can hang because of an undelivered signal.
	• Fixes a problem where if the size of the message queue was increased, writers to the queue that were blocked would not wake up for processing.
	• Provides the latest driver for the PowerStorm 4D10T (ELSA Gloria Synergy, SN-PBXGK-BB) graphics card.
	• Adds a fix to VMAC functionality when used with NETRain.
	• Fixes a problem where the following can occur during a system panic:
	– System calls interrupts.
	– mpsleep() returns an EINTR error when the panicstr is non-NULL.
	– An indefinite looping at a very high priority.
	• Corrects a problem with the incorrect ordering of network interfaces which was resulting in network partitions.
	• Updates the lfa ATM device driver to V1.0.17 and adds some enhancements as well as fixes a kernel memory fault seen when either shutting down or restarting the device driver.
	• Fixes a "lock_terminate: lock held" panic when deleting a process group.
	• Fixes an "unaligned kernel space access from kernel mode" panic when doing a malloc from kmembucket 26, 896 byte bucket. The faulting virtual address will be the lock signature for thread_deallocate().
	• Fixes a kernel memory fault in u_anon_faultpage() when it access the backing object for the anonymous page.
	• Fixes a problem where a root user was not allowed to check file access on behalf of a user without completely becoming the user. The functionality is needed by the ASU (Advanced Server for UNIX) product.
	• Fixes a panic in in_pcbfree() associated with ASE service failover.
	• Fixes a kernel memory fault seen under certain conditions when setting a thread's priority.
	• Includes UFS delayed metadata mount option that fixes metadata intensive application performance.
	• Fixes a race condition in the UBC code where a lookup is done on a page being invalidated (freed).
	• Fixes a race condition involving signals and threads that only happens on multiprocessor systems.
	• Fixes a problem when the type of SCSI device dynamically changes, which can result in a kernel memory fault or memory corruption panic.
	• Fixes a problem where the operating system only looks in slot 0 for the primary CPU.
	• Fixes a problem in which operations on NFS files can hang indefinitely.
	• Fixes a problem in AdvFS where putpage_lk/pg_busy deadlock causes hangs in the system.

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

Patch 1035.00 continued	• Corrects a problem when a network interface is configured using a CIDR bitmask and lies in a certain address range. It could be unreachable by users on the local system and remote systems that choose not to use the routing table, but simply transmit on an interface.
	• Fixes a "simple_lock: time limit exceeded" panic that can be seen on large configurations under a heavy load situation.
	• Fixes reply values for NFS writes that were causing protocol violations.
	• Fixes a simple lock panic.
	• Fixes a problem with cdfs. Fatal errors occur when trying to load data from a cdfs CD-ROM over NFS.
	• Corrects a problem which could cause the system to spend excessive time in the internet checksum routine, resulting in a degradation of system performance.
	• Fixes 2two network problems; a panic in in_pcbfree() when NFS is implemented over TCP, and a system hang with threads blocked in in_pcblock().
	• Fixes a panic in the UFS filesystem which has the following error message: blkfree: freeing free block
	• Fixes a hang or simple_lock_state_violation/simple_lock_fault panic in biodone.
	• This patch fixes two panics that have the following error messages: simple_lock: time limit exceeded simple_lock: lock already owned by cpu
Patch1037.00 OSF425-979B	**Patch:** Fixes reply values for NFS writes **State:** New This patch fixes reply values for NFS writes which were causing protocol violations.

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

Patch 1039.00 OSF425-1000	**Patch:** Security (SSRT0567U, SSRT0583U, SSRT0590U) **State:** New. Supersedes patches OSF425-400404-1 (45.01), OSF425-405233 (166.00), OSF425-405337-2 (349.02), OSF425-405470 (513.00), OSF425-405547 (531.00), OSF425-637 (669.00), OSF425-685 (707.00), OSF425-960 (1011.00) This patch corrects the following:

- Fixes the following problems with the at -t command:
  - The command did not work with user IDs that were not in the password file.
  - The command did not work on the leap year of 2000.
- Corrects several problems with the at, cron, and crontab commands.
- Fixes a problem with crontab where, when root runs crontab -e user, the user's crontab file is edited and saved, but is not reread by the cron daemon. Instead root's crontab file is reread.
- 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 some crontab jobs would run multiple times in the same minute.
- Fixes two cron problems:
  - The cron daemon does intensive logging and fills up the disk.
  - Multiple cron daemons continue to run and consume system resources due to the fact that, after a user is deleted from the system, there are still jobs running on the user's behalf.

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

Patch 1045.00 OSF425-974	**Patch:** Security (SSRT0546U, SSRT0542U, SSRT0641U) **State:** New. Supersedes patches OSF425-024 (1.00), OSF425-024-1 (1.01), OSF425-183 (110.00), OSF425-184 (90.00), OSF425-270 (199.00), OSF425-332 (248.00), OSF425-343-3 (258.03), OSF425-214 (112.00), OSF425-387-2 (296.02), OSF425-243-2 (181.02), OSF425-400434 (78.00), OSF425-400437 (68.00), OSF425-400437-1 (68.01), OSF425-063 (8.00), OSF425-063-1(8.01), OSF425-209 (101.00), OSF425-221 (168.00), OSF425-307 (230.00), OSF425-125 (6.00), OSF425-127 (13.00), OSF425-400435-1 (77.01), OSF425-405301 (341.00), OSF425-405389 (360.00), OSF425-405343 (350.00), OSF425-405422 (368.00), OSF425-128 (14.00), OSF425-400448 (75.00), OSF425-400448-1 (75.01), OSF425-163 (88.00), OSF425-405181 (160.00), OSF425-405217 (162.00), OSF425-193 (97.00), OSF425-299 (223.00), OSF425-353 (268.00), OSF425-358 (273.00), OSF425-363 (278.00), OSF425-309 (232.00), OSF425-344 (259.00), OSF425-405403-2 (362.02), OSF425-405520 (415.00), OSF425-464 (435.00), OSF425-405479 (515.00), OSF425-405528 (528.00), OSF425-405538 (529.00), OSF425-405564 (538.00), OSF425-410240 (551.00), OSF425-422 (555.00), OSF425-531A (582.00), OSF425-539A (588.00), OSF425-544 (590.00), OSF425-590 (614.00), OSF425-618 (653.00), OSF425-634 (666.00), OSF425-648 (678.00), OSF425-657 (686.00), OSF425-668 (694.00), OSF425-671 (696.00), OSF425-676 (700.00), OSF425-682 (705.00), OSF425-693 (714.00), OSF425-694 (715.00), OSF425-405586 (639.00), OSF425-405586 (639.00), OSF425-405586 (639.00), OSF425-727 (743.00), OSF425-758 (811.00), OSF425-780B (901.00), OSF425-800 (845.00), OSF425-801 (846.00), OSF425-874 (938.00), OSF425-806 (850.00), OSF425-912 (967.00), OSF425-914 (969.00), OSF425-942 (996.00), OSF425-954 (1006.00), OSF425-976 (1040.00), OSF425-966 (1041.00), OSF425-1018A (1042.00), OSF425-1015 (1043.00)

This patch corrects the following:

- Adds the contention scope attribute to the cma thread attributes list. The attribute sets the contention scope of the thread to be created.

- Fixes a problem that occurs when using the C shell (csh). When a command that does both wildcard expansion and command substitution is run in csh, incorrect results are produced.

- Fixes a problem in which the vquota, vedquota, quota, edquota, dump, csh, and nslookup commands will sometimes display incorrect error messages for non-English locales.

- Fixes a problem in which the dump command fails when the full patchname of the output file is not given.

- Fixes the problem that csh may omit the data byte 0x80 when processing a string in the ja_JP.SJIS or zh_TW.big5 locales.

- Fixes a problem with the quota command. When issuing a quota command the UID will be negative if the UID is greater than 16 bits.

- 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.

- Fixes problems that occur when using the ksh shell. When the PATH for a command is not found, the following error message is displayed. Also, when the set command is executed, the system core dumps.

  /bin/ksh: invalid multibyte character

- Fixes a problem in which the ksh command periodically prints erroneous characters instead of the command that was typed.

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

Patch 1045.00 continued	• Fixes a problem that occurs when using the Korn shell (ksh). Variables set with the typeset -L[n] built-in command do not work correctly when other subshells are spawned.
	• 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 carriage return) would cause the ksh utility to core dump.
	• 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 when built-in variables (for example, TMOUT) are exported as read only with values > 256. The set command (display all variables) will cause ksh to core dump with the error "stack overflow".
	• Corrects a problem that 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 TCP/IP problem that can occur with programs linked with the libc library. These programs may return a value of (-1) when calling the svc_tcp() function.
	• Fixes a problem with rexec(3) losing socket descriptors.
	• Corrects two problems:
	– A process hang when an application linked with libpthread performs a realloc(0,0).
	– A memory leak when small blocks are allocated with valloc().
	• Fixes a problem in which RPC client functions do not correctly handle system calls interrupted by a signal (EINTR errors).
	• Fixes a problem whereby exceptions propagating out of (or thrown from) __init routines in C (or C++) programs are not caught by the last-chance handler and result in an infinite loop.
	• Fixes a scanset processing problem in swscanf().
	• Fixes a memory leak in the libc glob() function.
	• Fixes a problem with printing floating-point values using the width and precision specifiers. Previously, the leading and trailing zero counts were often miscalculated.
	• 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

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

Patch 1045.00 continued	• Fixes a problem with strftime() when using width/precision modifiers with the %y field.
	• 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 problem whereby 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 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.
	• 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.
	• ksh does a segmentation fault and core dumps when displaying a here-document.
	• 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.

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

Patch 1045.00
continued

- Fixes a problem that may cause the malloc suite of functions to show heavy mutex lock contention in multithreaded applications running on multi-CPU systems.

- Introduces changes to the DECthreads libraries intended to improve the performance of threaded applications running on DIGITAL UNIX V4.0D. This patch specifically addresses the areas of thread scheduling, synchronization object performance and SMP scalability.

- 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(), swprint(), and fwprintf() do not handle the S format correctly. Instead of treating the data as logical characters, they treat data as bytes.

- Fixes a problem where C shell background processes started from within a terminal emulator window (dtterm, dxterm, or xterm) exit when the terminal emulator window is closed.

- 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 coredump when displaying a large here-document in a ksh script.

- Fixes a problem with the wcstod system call causing a core dump.

- Fixes problems with rsh(1), rlogin(1) rcp(1) if netgroup names are defined with capital letters.

- Fixes a problem with the Korn shell where data loss occurs when commnds are piped together.

- 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 V4.0D. The changes are related to synchronous signal processing and thread scheduling.

- Corrects how the C shell handles 2-byte characters when running in the Japanese SJIS locale.

- Fixes a problem of password error messages not being displayed during installation of the security subsystem.

- Fixes a problem in ksh which required two SIGTERM signals to be sent to the process when it exec'ed.

- 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.

- Fixes a problem in the C shell (csh) in which a segmentation fault will occur when the user defines an environmental variable that exceeds the 2048 character limitation. This limit has been lengthened to 8192 characters.

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

Patch 1045.00 continued	• Fixes a problem in ksh in which a space after the -p switch would cause the command to fail.
	• A potential security vulnerability has been discovered where, under certain circumstances users may gain unauthorized access. Compaq has corrected this potential vulnerability.
	• Increases the length of the user names for rsh and rexec to allow for NT interoperabilty.
	• Fixes a problem in ksh. When the current working directory is / and the command cd .. is entered, the following error message is displayed: ksh: ..: bad directory
	• Fixes a problem where gmtime() was erroneously setting the tzname[0] array.
	• Fixes a C shell problem where multibyte characters may not be displayed properly inside quotes.
	• Fixes a problem in libc that affects debugger tracebacks of code containing split procedures.
	• Adds functionality to termminate the resulting string from calls to swprintf().
	• Addresses performance and scalibility issues for highly contended threaded applications running on SMP machines.
	• Fixes a problem for those applications that assume initial allocations of memory from the C run-time library's malloc() function will return only zero-filled memory.
	• Fixes a getnetgrent(3) memory leak.
Patch 1047.00 OSF425-1018B	**Patch:** Security (SSRT0546U, SSRT0542U) **State:** New. Supersedes patches OSF425-343B (393.00), OSF425-407C (396.00), OSF425-405403C-2 (401.02), OSF425-539B (628.00), OSF425-582B (634.00) This patch fixes the following problems:
	• Hangs or unexpected termination of threaded processes with the TotalView debugger.
	• Gcc compiler reports errors when including the <pthread.h> header file.
	• 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.
	• Introduces changes to the DECthreads libraries intended to improve the performance of threaded applications running on DIGITAL UNIX V4.0D. 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.
	• Addresses performance and scalibility issues for highly contended threaded applications running on SMP machines

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

Patch 1049.00 OSF425CDE-031A	**Patch:** libDtSvc Fix, Security (SSRT0498U) **State:** New. Supersedes patches OSF425CDE-400013 (79.00), OSF425CDE-029A (912.00) 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 dtfile ICDE COSE tool does not work when TMPDIR is defined as /ldata/disk_local/tmp. dtfile returns this error: /ldata/disk_local/tmp/sdtdbcache_AAAaadmma: Cross-device link / ldata/disk_local/tmp/sdtdbcache_BAAaadmma: Cross-device link Floating exception (core dumped) • Fixes a problem with the Common Desktop Environment (CDE) in which some desktop applications will fail if CDE is not initialized. The error which appears in the user's home .dt/errorlog file is: Desktop Not Initialized: Could not createAction/Datatypes database.
Patch 1051.00 OSF425CDE-031B	**Patch:** Security (SSRT0498U) **State:** New. Supersedes patches OSF425CDE-400013B (172.00), OSF425CDE-029B (1017.00) 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 dtfile ICDE COSE tool does not work when TMPDIR is defined as /ldata/disk_local/tmp. dtfile returns this error: /ldata/disk_local/tmp/sdtdbcache_AAAaadmma: Cross-device link / ldata/disk_local/tmp/sdtdbcache_BAAaadmma: Cross-device link Floating exception (core dumped) • Fixes a problem with the Common Desktop Environment (CDE) in which some desktop applications will fail if CDE is not initialized. The error which appears in the user's home .dt/errorlog file is: Desktop Not Initialized: Could not createAction/Datatypes database.
Patch 1053.00 OSF425-987	**Patch:** Prevents not currently mounted warning message **State:** New This patch prevents "not currently mounted" warning messages from being displayed for filesystems you did not request to unmount.

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

Patch 1055.00 OSF425-994	**Patch:** Fixes limitation problem with grep and fgrep cmds **State:** New. Supersedes patches OSF425-933 (987.00), OSF425-937 (991.00) This patch corrects the following: • Corrects a problem with the fgrep command. When it is used with the -s flag all output is suppressed. • Fixes a limitation problem with the grep and fgrep commands. If the line length is too long, grep displays a "wordlist too large" error message and fgrep displays "input too long" error message. • The command fgrep -f searchlist gets the following error message: wordlist too large if the searchlist is too long. In the test case it was 1500 entries. • The command fgrep -f searchlist displays datafiles verbatim if the searchlist has blank lines.

Patch 1057.00
OSF425-1006
	Patch: Fixes problem with tar command
	State: New. Supersedes patches OSF425-130 (15.00), OSF425-162 (31.00), OSF425-181 (42.00), OSF425-181-1 (42.01), OSF425-210 (104.00), OSF425-414-1 (316.02), OSF425-573 (602.00), OSF425-646 (676.00), OSF425-945 (998.00)
	
	This patch corrects the following:
	
	• Fixes a problem in which /usr/bin/pax : cpio -pl does not link files when possible, but copies them.
	
	• Fixes a problem with the tar and pax programs. These programs incorrectly append files to an existing archive and cause the file to become corrupt.
	
	• Fixes pax's tar and cpio archive handling to allow filesizes greater than 4GB.
	
	• Corrects the problem where tar dumps core when trying to untar a compressed archive.
	
	• 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 occured in the following cases:
	
	  – If the file was a non-empty directory.
	
	  – If the file was the target of another symbolic link.
	
	• Fixes a cpio hanging problem in the Japanese locales.
	
	• Fixes a problem with the tar command. Corruption occurs when restoring a file system that contains more than two hard links to a file.

Patch 1059.00 OSF425-983	**Patch:** Fix for lastlogin command **State:** New This patch resolves the Y2K problem of lastlogin command incorrectly calculating the last date each user logged in.

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

Patch 1061.00 OSF425-968	**Patch:** Corrects slow shutdown **State:** New This patch corrects slow shutdown due to name lookups deleting routes.
Patch 1063.00 OSF425-986	**Patch:** Security (SSRT0546U, SSRT0542U, SSRT0636U) **State:** New. Supersedes patches OSF425-405403B-2 (400.02), OSF425-405568 (540.00), OSF425-405569 (541.00, OSF425-882 (944.00) 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. • Fixes a problem where named could possibly core dump when printing an informational message to syslog.

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

Patch 1065.00
OSF425DX-039

Patch: Corrects date and time stamp for new user id

State: New. Supersedes patches OSF425DX-007 (153.00), OSF425DX-405008 (379.00), OSF425DX-011 (328.00), OSF425DX-015 (332.00), OSF425DX-016 (333.00), OSF425DX-002-2 (336.02), OSF425DX-025 (749.00), OSF425DX-028 (750.00), OSF425DX-029 (751.00), OSF425DX-405010 (510.00), OSF425DX-031 (752.00), OSF425DX-032 (780.00), OSF425DX-035 (914.00), OSF425DX-037 (916.00), OSF425DX-038 (917.00), OSF425DX-008 (152.00), OSF425DX-017 (334.00), OSF425DX-013-2 (330.02), OSF425DX-036 (915.00)

This patch fixes the following problems:

- Fixes the following problems encountered when using the Account Manager application (dxaccounts):

  – When you move an accounts home directory, symbolic links in the old home directory are resolved and files pointed to by the links are copied into the new home directory.

  – The userdel utility core dumps when attempting to delete a user account that is running enhanced C2 security.

  – When modifying an existing NIS "+" or NIS "-" user account by turning off the NIS Overrides toggle, the User ID field is incorrectly set to 0.

- 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 where dxaccounts allows the colon (:) character to be accepted in the user shell, home directory, fullname, office, office phone, and home phone fields. This caused the /etc/passwd file to become corrupted.

- 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 the following problems:

  – userdel does not remove accounts from the /etc/passwd file. The userdel command displays an error message stating the /etc/passwd file is corrupted, when in fact it is not.

  – dxaccounts application does not allow users to be added to groups with group ID lower than the default minimum specified in the General Options dialog.

  – Files in subdirectories in the /usr/skel directory are not copied properly to the newly created user's home directory.

- Fixes a problem that causes the account management commands (dxaccounts, useradd, and usermod) to split long NIS group lines incorrectly. This causes a majority of users to have improper access to files, directories, and applications and also causes the newgrp command to fail.

- 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 two situations in which the GUI account management program (dxaccounts) will crash in a Enhanced Security client environment when attempting to copy a NIS user account.

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

Patch 1065.00 continued	• 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 are filled.
	• 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.
	• Updates the error message displayed when Account Manager fails to start due to the detection of an Account Manager lock file (/etc/.AM_is_running) on the system.
	• Fixes a problem in which dxaccounts does not allow the system manager to add NIS users when the system is running enhanced security.
	• Fixes the problem of enabling to change root's login/uid through cli/dxaccounts utilities.
	• When issuing a useradd -D or usermod -D command to view the account manager defaults, the Inactive (days) value would always show the character s rather than nothing when the Inactive days status has been defeated with a -1 value.
	• Fixes the problem where usermod -g <group> <user> will lock the user account if it is unlocked.
	• Fixes a problem where adding a 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 in which a command usermod -D does not display the Expire date when it is set.
	• Fixes a problem where the new home directory for a new user id is created with the date and time stamp of the /usr/skel directory.

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

Patch 1069.00 OSF425X11-035A	**Patch:** CDE Fixes, Security (SSRT0547U)
	State: New. Supersedes patches OSF425X11-005 (155.00), OSF425X11-405011-3 (382.03), OSF425X11-012 (754.00), OSF425X11-400020 (56.00), OSF425X11-405009 (171.00), OSF425X11-405010-3 (381.03), OSF425X11-011A (753.00), OSF425X11-405016A (546.00), OSF425X11-014A (756.00), OSF425X11-017A (782.00), OSF425X11-021A (785.00), OSF425X11-028A (923.00), OSF425X11-033A (1066.00), OSF425X11-034A (1067.00)

This patch fixes the following problems:

- When managing a CDE session on an X terminal from a DIGITAL UNIX system, and the X terminal does not perform a normal logout, some of the CDE processes on the DIGITAL UNIX system are left running.

- A potential security vulnerability has been discovered where, under certain circumstances, users may gain unauthorized access. Compaq has corrected this potential vulnerability.

- Fixes a problem in the X Display Manager (xdm) where XDMCP Indirect queries do not work.

- Fixes various Minor System Faults (MSFs) in the X Toolkit library (libXt).

- Fixes the memory leak in the Motif text widget when changing colors using XtVaSetValues().

- Fixes a small memory leak in the Motif text widget.

- Fixes the Motif tear-off menu core dump problem. The problem is seen when the tear-off menu from a pull-down 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.

- Provides suppport in the X11 Environment for the Euro currency symbol using the UTF-8 Unicode locales.

- 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".

- 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.

- Prevents a potential core dump from the X11 library when running an input method server for Japanese, Chinese, or Korean.

- Fixes various memory leaks in the X Window System's X Toolkit library (Xt) that could occur when creating and destroying Motif List, Text, and TextField widgets.

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

Patch 1073.00 OSF425X11-035B	**Patch:** Security (SSRT0547U) **State:** New. Supersedes patches OSF425X11-005 (155.00), OSF425X11-405011 (382.00), OSF425X11-405011B-2 (412.02), OSF425X11-400020 (56.00), OSF425X11-405009 (171.00), OSF425X11-405010 (381.00), OSF425X11-405010B-2 (411.02), OSF425X11-011B (772.00), OSF425X11-405016B (624.00), OSF425X11-014B (775.00), OSF425X11-017B (895.00), OSF425X11-021B (896.00), OSF425X11-028B (1021.00), OSF425X11-033B (1070.00), OSF425X11-034B (1071.00)

This patch fixes the following problems:

- When managing a CDE session on an X terminal from a DIGITAL UNIX system, and the X terminal does not perform a normal logout, some of the CDE processes on the DIGITAL UNIX system are left running.

- A potential security vulnerability has been discovered where, under certain circumstances, users may gain unauthorized access. Compaq has corrected this potential vulnerability.

- Fixes a problem in the X Display Manager (xdm) where XDMCP Indirect queries do not work.

- Fixes various Minor System Faults (MSFs) in the X Toolkit library (libXt).

- Fixes the memory leak in the Motif text widget when changing colors using XtVaSetValues().

- Fixes a small memory leak in the Motif text widget.

- Fixes the Motif tear-off menu core dump problem. The problem is seen when the tear-off menu from a pull-down 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.

- Provides suppport in the X11 Environment for the Euro currency symbol using the UTF-8 Unicode locales.

- 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".

- 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.

- Prevents a potential core dump from the X11 library when running an input method server for Japanese, Chinese, or Korean.

- Fixes various memory leaks in the X Window System's X Toolkit library (Xt) that could occur when creating and destroying Motif List, Text, and TextField widgets.

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

Patch 1076.00 OSF425-1016	**Patch:** Upgrades sys_check utility to v119 **State:** New. Supersedes patches OSF425-580 (607.00), OSF425-849 (887.00), OSF425-807 (851.00), OSF425-1020 (1074.00) This patch corrects the following:

- Updates sys_check utility to version V111.

- Provides the following changes to the sys_check utility:

  – Fixes the ra200info tool from core dumping.

  – Updates the sys_check utility to revision 114.

- Provides a new collection information tool used by the sys_check utility.

- 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.

  – Fixes several problems with the collect command and adds sysloging when collect suspends, resumes, or receives a signal.

  – Upgrades sys_check utility to v119 and provides the following changes:

    ☐ Fixes the ra200info tool from core dumping.

    ☐ Utilizes Compaq Analyze when available.

    ☐ Utilizes storage's new cliscript tool in place of hszterm.

    ☐ Updates ASU section.

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

Patch 1086.00	**Patch:** Fixes an AdvFS panic
OSF425-989	**State:** New. Supersedes patches OSF425-061 (82.00), OSF425-135 (21.00), OSF425-169 (36.00), OSF425-410118 (51.00), OSF425-180 (41.00), OSF425-400443 (67.00), OSF425-157 (81.00), OSF425-157-1 (81.01), OSF425-194 (93.00), OSF425-197 (96.00), OSF425-205 (124.00), OSF425-207 (123.00), OSF425-215 (115.00), OSF425-219 (113.00), OSF425-224 (129.00), OSF425-234 (130.00), OSF425-237 (133.00), OSF425-241 (135.00), OSF425-251 (144.00), OSF425-232 (127.00), OSF425-238 (138.00), OSF425-239 (148.00), OSF425-244 (139.00), OSF425-247 (183.00), OSF425-257 (188.00), OSF425-262 (192.00), OSF425-275 (204.00), OSF425-276 (205.00), OSF425-281 (209.00), OSF425-292 (217.00), OSF425-301 (225.00), OSF425-305 (228.00), OSF425-315 (235.00), OSF425-321 (240.00), OSF425-327 (243.00), OSF425-359 (274.00), OSF425-371 (285.00), OSF425-385 (294.00), OSF425-395 (301.00), OSF425-401 (306.00), OSF425-404 (308.00), OSF425-406 (309.00), OSF425-437 (324.00), OSF425-279 (208.00), OSF425-370 (284.00), OSF425-249B (385.00), OSF425-296B (386.00), OSF425-320B (387.00), OSF425-360B (388.00), OSF425-418B (389.00), OSF425-362B (390.00), OSF425-410B (391.00), OSF425-278B-2 (392.02), OSF425-429 (556.00), OSF425-430 (557.00), OSF425-436 (558.00), OSF425-450 (560.00), OSF425-451 (561.00), OSF425-453 (562.00), OSF425-454 (563.00), OSF425-459 (565.00), OSF425-461 (566.00), OSF425-462 (567.00), OSF425-470 (568.00), OSF425-473 (569.00), OSF425-479 (570.00), OSF425-481 (571.00), OSF425-493 (573.00), OSF425-498 (574.00), OSF425-504 (575.00), OSF425-513 (576.00), OSF425-514 (577.00), OSF425-516 (578.00), OSF425-519 (579.00), OSF425-538 (587.00), OSF425-539C (629.00), OSF425-540 (589.00), OSF425-547B (630.00), OSF425-555 (595.00), OSF425-559 (596.00), OSF425-576 (605.00), OSF425-597 (617.00), OSF425-537B (637.00), OSF425-586B (638.00), OSF425-354-2 (269.02), OSF425-405320 (344.00), OSF425-405408-2 (366.02), OSF425-625 (660.00), OSF425-632 (664.00), OSF425-640 (671.00), OSF425-644 (674.00), OSF425-645 (675.00), OSF425-647 (677.00), OSF425-649 (679.00), OSF425-689 (711.00), OSF425-701 (721.00), OSF425-704 (724.00), OSF425-713 (731.00), OSF425-715 (733.00), OSF425-720 (738.00), OSF425-447B (625.00), OSF425-729 (745.00), OSF425-630B (764.00), OSF425-654B (765.00), OSF425-631 (787.00), OSF425-669 (788.00), OSF425-747 (801.00), OSF425-753 (806.00), OSF425-760 (812.00), OSF425-768 (818.00), OSF425-769 (819.00), OSF425-786 (833.00), OSF425-793 (839.00), OSF425-796 (841.00), OSF425-808 (852.00), OSF425-823 (865.00), OSF425-825 (867.00), OSF425-832 (873.00), OSF425-850 (888.00), OSF425-686B (767.00), OSF425-851 (889.00), OSF425-692B (897.00), OSF425-750B (899.00), OSF425-775B (900.00), OSF425-797B (902.00), OSF425-816B (903.00), OSF425-860 (929.00), OSF425-869 (935.00), OSF425-870 (936.00), OSF425-883 (945.00), OSF425-887 (947.00), OSF425-893 (950.00), OSF425-902 (957.00), OSF425-916 (971.00), OSF425-918 (973.00), OSF425-926 (980.00), OSF425-938 (992.00), OSF425-956 (1008.00), OSF425-857 (927.00), OSF425-910B (1023.00), OSF425-889 (948.00), OSF425-990 (1077.00), OSF425-1014 (1078.00), OSF425-1002 (1079.00), OSF425-1004 (1080.00), OSF425-999 (1081.00), OSF425-1001 (1082.00), OSF425-985 (1083.00), OSF425-1009 (1084.00)

- Corrects a problem with an NFS V3 mounted AdvFS file system where, under heavy I/O load, data being written to a file may be lost. Additionally, because file stats are not being saved, the file modification time may revert to a previous value.

- Provides a performance improvement for AdvFS systems.

- Corrects a problem in AdvFS where a data structure field is not initialized until after an AdvFS mount, which is too late. This results in the inability, for example, to see the files after a remount.

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

Patch 1086.00 continued	• Fixes a problem that occurs on SMP systems with an AdvFS filesystem in which the system panics with the following message:

simple_lock: time limit exceeded

• Fixes a problem with the vrestore command. When restoring a multivolume tape archive, if the tapes that follow the first tape are write-protected, the following error message is displayed:

vrestore: can't open device file

• Fixes a problem caused by the vdump command. When a user entered Ctrl/C to terminate a vdump operation, the command returned an incorrect status and mistakenly updated the /etc/vdumpdates file.

• Fixes a problem that occurred when an AdvFS panic crashed the system but the visible symptom was a crash due to a kernel memory fault.

• Fixes a problem with the chfsets command. When a root user exceeded the fileset quota (which root is allowed to do), the chfsets command reported negative values for the free and available blocks in the fileset.

• Fixes a problem with AdvFS in which the following panic occurs:

clone: str_stripe_clone err

• Modifies the vd_remove() function to set domain panic instead of panicing the system.

• Fixes a problem that crashed the system while it was running a collision test. The process would hang on a lock, never be woken, and crash the system.

• Fixes an AdvFS problem that occurs when unmounting a domain. An unmount thread was waiting on a variable to be set to zero before continuing, but the routine that was to set the variable to zero never did.

• Fixes a problem with the AdvFS fs_write routine, which would mishandle partial writes after detecting an error.

• Corrects a problem where a panic would occur when running rmtrashcan on a clone.

• Fixes a problem with AdvFS which caused a system panic with the following message:

log_flush_sync: pingpg error

A system panic occurred when the AdvFS domain had already issued a domain panic and a user application then attempted to close a file in that domain.

• Fixes a problem with AdvFS which would corrupt a clone fileset when it truncated the original fileset.

• Provides performance improvements for writes to AdvFS files which have had Atomic Write Data Logging enabled on them. Write performance improvements are for O_SYNC opens of such files and are realized for both local and NFS access.

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

Patch 1086.00 continued	• Fixes a problem in AdvFS that produced the following system panic: bs_logflush_start: cannot write lsn • Fixes a problem with messages in system logs that reported AdvFS user and group quota limits. The messages were unclear; the user could not determine from them which users or groups were reaching the quota limits. • Fixes several problems associated with AdvFS tag files and directories, including displays of erroneous data and system panics. • Fixes a problem in AdvFS locking code which causes the following panic: kernel memory fault • Fixes a problem in AdvFS that causes a system panic when a truncate operation is performed on a file. The panic is: log half full • Fixes a problem in AdvFS that was causing a memory leak. • Fixes the following problems in AdvFS: – AdvFS does not return an error when a user opens a file in O_SYNC mode and power is lost on the disk drive. – A locking error in the AdvFS fs_write() routine. • Fixes a problem with AdvFS that caused a page fault and the following panic: panic (cpu 0): kernel memory fault • Fixes two AdvFS problems: – An error message was misleading when a DIGITAL UNIX Version 4.0 system attempted to access a file domain created by Tru64 UNIX Version 5.0. – A state field in an AdvFS data structure was initialized, but not maintained. • Fixes a problem where user files or the AdvFS frag file could lose data if they are updated during an AdvFS migration (that is, during a balance, defragment, migrate, or rmvol of their AdvFS domain).

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

Patch 1086.00 continued	• 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 three verify command problems:
	– The command was displaying a large volume of meaningless data.
	– When it encountered a nonrecoverable error, the command did not properly exit.
	– The command sent some error messages to stderr, some to stdout.
	• 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 with AdvFS, which produced the following error while attempting to migrate a sparse file:
	E_CANT_MIGRATE_HOLE
	• Fixes the following problems in the AdvFS system:
	– The log file corruption caused panics during recovery and failures and displayed one of the following messages:
	ftx_fail: lgr_read failure
	ftx_fail: dirty page not allowed
	kernel memory fault
	can't clear a bit twice
	can't set a bit twice
	Note: This only fixes a subset of the known set/clear bit panics.
	• Fixes a problem in the AdvFS logging code, The way locking was implemented was causing degraded performance.
	• Corrects an I/O subsystem performance bottleneck. A system which experiences periodic system slowdowns may need this patch.
	• Fixes an operating system hang condition. The hang condition exists due to processes deadlocking in the AdvFS code.
	• Fixes a problem with AdvFS performance. The patch provides a performance improvement to the msync system call when it is called for an AdvFS mmapped file.
	• Fixes an AdvFS problem that occurs when the rmvol command is stopped before the commmand successfully removes a volume from a domain. As a result, the showfdmn and addvol commands interpreted the volume as still in the domain (although with no data available) and a balance operation returned the following AdvFS error message:
	get vol params error EBAD_VDI (-1030)

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

Patch 1086.00 continued	• Fixes a problem with the defragment command, where the -V option is not being parsed properly.
	• Fixes a problem in AdvFS that produced the following system panic:
	malloc_overflow: guard space corruption
	• Fixes a problem with the vdump command, which was modifiying the atime file attribute whenever files were backed up, thereby eliminating the ability to determine when the files were last accessed by a user.
	• Enhances the AdvFS verify utility to detect incorrect holes in frags file.
	• Fixes an AdvFS problem which can allow I/O requests to bypass the ready lazy queue.
	• Fixes a problem in the AdvFS system. The system hangs due to a deadlock between update daemon sync() syscall processing in AdvFS and the truncation of AdvFS file.
	• 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.
	• 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 observed when using the edquota command under the Advanced File System (AdvFS). The edquota command may display an incorrect grace period.
	• This patch applies to AdvFS use only and corrects a problem whereby rmvol(8) will not remove multiple stripes of the same file on a volume. The error code EBAD_VDI (-1030) may be displayed.
	• 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.
	• Fixes two AdvFS problems:
	– When an AdvFS volume is nearly full, AdvFS files may become corrupt as they are closed. The verify utility can be used to detect this overlapped frag corruption problem.
	– The truncation of the fragment bitfile was erroneously being turned off. This feature allows AdvFS to give back disk space periodically.
	• Fixes a panic in the AdvFS system. The panic has the following error message:
	lock_read: hierarchy violation

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

Patch 1086.00 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 potential problem with the vdump command.
- 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.
- This enhancement for the /sbin/advfs/verify utility allows it to detect loops in the list of free frags kept in the frags file.
- 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.
- Makes vrestore work with QIC-120 and QIC-150 tapes.
- Fixes an AdvFS hang that is caused by a deadlock between the_XentMM() and msfs_mmap() system calls.
- Fixes a problem in which a system can hang because cleanup_closed_list() can go into a loop.
- Introduces changes to the DECthreads libraries intended to improve the performance of threaded applications running on DIGITAL UNIX V4.0D. This patch specifically addresses the areas of thread scheduling, synchronization object performance and SMP scalability.
- 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".
- Fixes a problem in AdvFS which could cause thread hangs or a system panic.
- 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 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 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).

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

Patch 1086.00 continued	• Fixes the following problems:

• 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 multi-CPU systems, hangs can occur in the revoke system call when multiple threads attempt to call revoke at the same time.

• Fixes a problem where several processes accessing the same AdvFS file can hang in ubc_lookup().

• 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.

• Fixes a problem where the vdump program would dump core with the following message:

nnnn Resources lost(coredump)

• 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.

• Corrects a problem that caused invalid fragment information to be reported for an AdvFS file. The invalid information was returned in response to a verify command.

• 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 in which the system panics due to AdvFs lock hierarchy violation.

• Fixes a problem with the defragment command. Prior to this patch the defragment command could fail and display inacurate error descriptions. The problem was caused by uninitialized variables for the command.

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

Patch 1086.00 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 is:
	
	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 system crashes during rmdir.
	
	• Fixes the problem where the system panics whenever nextFlushSeq reaches the max. This fix allows nextFlushSeq (and other buffer lsn's) to roll over.
	
	• 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.
	
	• Fixes the following two problems in AdvFS:
	
	  – When a "log half full" or "log full" problem occurs, an entire system will panic.
	
	  – The error 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 precedes each log record in a log page.
	
	• 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.
	
	• 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
	
	• Corrects some error messages given when the AdvFS utility verify(8) detects file errors. It also corrects a problem whereby verify was unable to delete files with no directory entries.
	
	• Ensures all AdvFS root fileset buffers are flushed on shutdown.
	
	• 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.
	
	• 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()

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

Patch 1086.00 continued	• 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
	• Fixes a problem in which it prevents a system panic if str_stripe_clone returns an error.
	• Fixes two problems with the vrestore command: – 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. In addition this patch corrects intermittent failures to display archive records for the above files (compressed or not) when the list option was selected.
	• Avoids corruption of a filesystem when verify runs with -r & -f flags on an active domain. Verify returns usage message when -r flag is used with either -f or -dFixes 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 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 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
	• 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.

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

Patch 1086.00 continued	• Corrects two problems in AdvFS property list handling:

• 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.

• Fixes a problem with the parameter checking code of the fcntl system call. As a result, incorrectly coded fcntl() parameters in user programs no longer panic the system.

• Fixes the AdvFS race between extending and reading subextent maps and avoids the panic occured in AdvFS bs_get_bf_xtnt_map code (QAR 61985). This patch also fixes the race with removing storage causing kernel memory fault (QAR 66890).

• Fixes a panic in AdvFS which can have the following error messages:

panic (cpu 1): bs_cow_pg: pin clone err

panic (cpu 1): bs_cow_pg: cannot get blkMap

• 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 problem in which an invalid error status is returned from the remove_entry system call.

• Fixes a problem in AdvFS. The system panics with a kernel memory fault.

• Fixes a problem in AdvFS. A system panic occured with the following error message:

panic: del_dealloc_stg(): cant ref bmt page

• Fixes the following /sbin/advfs/verify command problems:

   – Verify fails to complete on a large number of files.

   – Verify will core dump when an offset into mountd[] array that is used to pull out the fileset name is corrupted.

   – Verify incorrectly reports errors on BMTs that have multiple extent records for domains created with the mkfdmn -p switch.

   – Verify fails when lseeking on very large domains.

• Fixes a problem that caused AdvFS to incorrectly calculate metadata file size for files greater than 4GB resulting in corruption on read and stat syscalls.

• Fixes a problem where the output of a ps command, the PAGEIN column reports 0 for all processes.

• Fixes a problem in AdvFS. A panic occurs with the following error message:

lock_read: hierarchy violation

• Fixes AdvFS inconsistent quota problems and errors similar to the following appearing on the console:

vmunix: chk_bf_quota: group quota underflow

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

Patch 1086.00 continued	• Fixes a problem with verify. When verify is run on a brand new domain, nfs warnings are displayed even though no nfs related activity is being done.
	• Fixes a system hang that could last up to a few minutes with large files when performing synchronous IO requests.
	• Fixes an AdvFS problem which caused the system to crash with a kernel memory fault.
	• Fixes a problem with a kernel memory fault in AdvFS.
	• Fixes a problem in which the chfile utility returns an incorrect error code.
	• Fixes a problem in AdvFS where putpage_lk/pg_busy deadlock causes hangs in the system.
	• Fixes the following vrestore problems:
	– A previous patch caused incomplete restores.
	– A warning message is displayed when the path for the first file in a group of hardlinks is created without using original protection codes and property lists.
	– A warning message is displayed and vrestore aborts if it fails to malloc space for a property list.
	– A message which had been inserted at the end of the message file had the wrong message category (this could cause messaging confusion).
	– An uninitialized variable in the code that restores property lists could cause malloc failures, memory faults, an "error setting extended attributes" message, and infinite loops using the -l option.
	– Corrupted property list information could cause an infinite loop.
	• Fixes an AdvFS kernel memory fault caused by a race condition between migrate and chfile -L in bfflush_start.
	• Fixes a problem in AdvFS. The following error messages can occur:
	panic: simple_lock: uninitialized lock
	kernel memory fault: simple_lock: minimum spl violation
	• Fixes a problem in AdvFS in which a system that had already domain paniced results in a system panic.
	• Fixes a problem where the vdump command will sometimes store symbolic link files as directories in the vdump archive.
	• Fixes a problem where an AdvFS domain becomes inaccessible when using the mount -d option.
	• Fixes a problem with AdvFS in which a hang occurs due to a deadlock between bsbuf.state and bmt extent map lock.
	• Fixes a problem with AdvFS where all processes are waiting for buffers, causing the system to hang.
	• Fixes a problem in AdvFS where user data may be lost when a clone file is migrated.
	• This patch fixes a panic in AdvFS with the following error message:
	ftx_fail_2: dirty page not allowed

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

Patch 1089.00 OSF425-998	**Patch:** Various fixes for printer problems **State:** New. Supersedes patches OSF425-123 (61.00), OSF425-123-1 (61.01), OSF425-405157 (158.00), OSF425-405295-3 (398.03), OSF425-438 (399.02), OSF425-589 (613.00), OSF425-698 (719.00), OSF425-711 (729.00), OSF425-811 (855.00), OSF425-821 (863.00), OSF425-894 (951.00), OSF425-903 (958.00), OSF425-984 (1015.00), OSF425-1021 (1087.00)

This patch corrects the following:

- Fixes a problem where the lpq command causes the program to crash (memory fault).

- Fixes a problem with the lpd line printer daemon. When /sbin/init.d/lpd stop, is followed right away by /sbin/init.d/lpd start, the new lpd fails to start. The error message from syslog is:

  /usr/spool/lpd.lock: locking failed: Operation would block

- Fixes to improve the reliability and efficiency of DIGITAL UNIX print services.

- Provides support to the BSD lpd(8) print system for DIGITAL UNIX Advanced Printing System (APX).

- Fixes a problem where, under certain circumstances, a print queue becomes disabled and printing stops.

- Provides printer support for the Euro currency symbol provided in the UTF-8 Unicode locales.

- When printing jobs, a timeout can occur after 5 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.

- Fixes a problem where some print jobs will print out twice.

- Fixes a problem where 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.

- When using the I18N ya option, the queue daemon filters will terminate after 32 jobs.

- Under certain circumstances, print jobs are terminated when printing to certain printers that are connected to a DECserver through TCP/IP.

- Fixes a problem with the lpstat -u command output.

- Fixes a printing problem where lpd reads any data from the printer that has not been read for local and remote connections. The read-backs for remote connections cause an addtional two second timeout which may cause a job-submit failure on the job-number wraparound.

- Corrects a problem in which, under certain conditions, unnecessary error messages are written to the lpr.log file.

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

Patch 1089.00 continued	• A user is unable to delete a print job from a remote system with a hostname greater than 32 characters because the hostname was truncated.
	• When a TCP/IP connection fails, the retry algorithm would take longer to print jobs due to a long retry interval.
	• A timing hole during lpd last-job completion and shutdown needed to be closed.
	• It was not possible to print to the lpd queue using Windows 2000.
Patch 1091.00 OSF425-981	**Patch:** advscan Command Correction **State:** New. Supersedes patches OSF425-405263 (338.00), OSF425-405359-1 (352.01) This patch fixes the following problems:
	• Fixes a problem caused by the advscan -r command. The command would link LSM volumes to the raw device instead of the block device when it attempted to recreate LSM volume links. As a result, the directory for the domain name in the /etc/fdmns file was incorrect and data corruption occurred.
	• Fixes a problem in which the advscan -a command causes a memory fault (core dump) while processing LSM volumes.
	• Fixes a problem where advscan -a -g does not display bootable partitions properly.
Patch 1094.00 OSF425-1013	**Patch:** Fix for mv command **State:** New. Supersedes patches OSF425-927 (981.00), OSF425-1008 (1092.00) This patch fixes the following problems with the mv command:
	• An invalid error message appears when attempting to move files in which the source name is the same as the destination name.
	• Using mv -i to rename a symlink pointing to a file on a different filesystem owned by a different user results in the prompt: Ownership of y will change. Continue?
	• When moving a file from one filesystem to another, the mv command will copy the file rather than using the rename() system call. This can result in file loss.
	• Corrects the problem with the mv(1) command deleting files in the directory when the user moves a directory to itself.

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

Patch 1096.00 OSF425CDE-032	**Patch:** Security (SSRT0571U) **State:** New. Supersedes patches OSF425CDE-405011-2 (376.02), OSF425CDE-405014 (505.00), OSF425CDE-405022 (508.00), OSF425CDE-011 (553.00) 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 the problem where dtmail corrupts binary attachments that are sent as Sun Mail Tool attachments. • 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. • Fixes a dtmail problem in which a From line with quotes in it incorrectly finds the date of the mail message. This error is displayed on the main screen under the header Date and Time and shows up as Dec. 31 or as a blank field.
Patch 1098.00 OSF425CDE-035	**Patch:** dtwm hangs on system using multiple displays **State:** New. Supersedes patches OSF425CDE-004 (151.00), OSF425CDE-005-2 (326.02) This patch corrects the following: • Fixes a problem in which the Desktop Window Manager (dtwm) causes a segmentation fault when users try to log into CDE. This can occur if the user has disabled personal customization of items on the CDE front panel via the LOCKED True statement in a dtwm.fp file. • Fixes a problem in which deleting applications (icons) from some subpanels hangs the CDE Window Manager. The subpanels affected are Calendar, Mail, and Desktop Style subpanels. • Fixes a problem in which the Window Manager (dtwm) intermittently hangs on a system which uses multiple displays.
Patch 1100.00 OSF425-973	**Patch:** Fix for tapex utility **State:** New This patch fixes several problems in the tapex utility. Accuracy of performance tests has been improved, the tapex exit status has been corrected, and tapex was fixed to determine eom status in Command Timeout Test and exit with non-0 status to indicate failure.
Patch 1102.00 OSF425-1024	**Patch:** assembler generates incorrect error messages **State:** New This patch corrects a problem whereby the assembler would generate incorrect error messages for source programs which produce a mix of hand-coded and assembler-generated relocation operands.

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

Patch 1104.00 OSF425-980	**Patch:** DIGITAL UNIX LAT Correction **State:** New. Supersedes patch OSF425-400478-1 (76.01) This patch corrects the following: • When printing using DIGITAL UNIX LAT (V4.0 or later) to a printer connected to a PC running Pathworks, an "I/O error" message is displayed and nothing is printed. • Corrects a problem in the LAT driver which caused improper processing of the ioctl TCSBRK as well as the generation of spurious characters when the libc routine tcdrain() was used.
Patch 1106.00 OSF425-1003	**Patch:** Security (SSRT0587U) **State:** New. Supersedes patch OSF425-405311-2 (342.02) 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. • Corrects the problem so mailx(1) will work correctly if -r and -s flags are used together.
Patch 1109.00 OSF425CDE-034	**Patch:** Security (SSRT0600U) **State:** New. Supersedes patches OSF425CDE-018 (636.00), OSF425CDE-014 (758.00), OSF425CDE-016 (760.00), OSF425CDE-033 (1107.00) 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. • Fixes a problem where the Common Desktop Environment (CDE) login daemon, dtlogin, core dumps occasionally when servicing requests from XDMCP clients such as X terminals or PCs running X servers. • Fixes a problem with the Common Desktop Environment (CDE) login process where, if you selected the Command Line Login option and logged in, sometimes the CDE login screen would be redisplayed before you had logged out.
Patch 1100.00 OSF425-1011	**Patch:** Fix for what command **State:** New. The what command was unable to process more than one input file at a time.
Patch 1113.00 OSF425-970	**Patch:** Fix for SysV Open call audit parameter **State:** New This patch fixes a problem where encoding for the SysV Open call audit parameter was incorrect. This could cause a system panic.

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

Patch 1116.00 OSF425-1005A	**Patch:** Security (SSRT0588U, SSRT0642U) **State:** New. Supersedes patches OSF425-182 (85.00), OSF425-405349-2 (351.02), OSF425-433A (424.00), OSF425-524A (451.00), OSF425-725A (742.00), OSF425-820A (862.00), OSF425-852A (890.00), OSF425-924A (979.00), OSF425-859A (928.00), OSF425-971A (1114.00)

This patch fixes the following problems:

- Fixes a problem with Enhanced Security not handling a voucher correctly from some other security mechanism such as DCE. The scenario to reproduce the problem is as follows:

  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 message "login incorrect".

- 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.

- Fixes a problem with logins in a DCE/C2 environment. The user could encounter an error "Bad priority setting" if there is a u_priority setting used in /etc/auth/system/default file.

- Corrects a problem with the rsh command displaying a warning message instead of the rsh command output when C2 security is configured.

- Fixes a problem when a system is configured with DECnet, C2 and NIS. When invoking edauth(8) <user_name>, the error: "Must be on NIS master server to update entry for <user_name>" is returned.

- Fixes a problem for Enhanced Security configurations where the Maximum Login Interval (u_max_login_intvl) field was being ignored for account templates.

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

Patch 1119.00 OSF425-1005B	**Patch:** Security (SSRT0588U, SSRT0642U)
	State: New. Supersedes patches OSF425-182B-2 (176.02), OSF425-433B (425.00), OSF425-524B (452.00), OSF425-725B (771.00), OSF425-820B (905.00), OSF425-852B (906.00), OSF425-859B (1022.00), OSF425-971B (1117.00)
	This patch fixes the following problems:
	• 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.
	• Fixes a problem with logins in a DCE/C2 environment. The user could encounter an error "Bad priority setting" if there is a u_priority setting used in /etc/auth/system/default file.
	• Corrects a problem with the rsh command displaying a warning message instead of the rsh command output when C2 security is configured.
Patch 1121.00 OSF425DX-040	**Patch:** diskconfig issues error message at startup
	State: New
	This patch fixes a problem that was causing diskconfig to issue the error message "can't read tminor: no such variable" upon startup.
Patch 1123.00 OSF425-1042	**Patch:** Fix for FDI floppy driver
	State: New. Supersedes patch OSF425-763 (814.00)
	This patch fixes a problem in the FDI floppy driver. A recursion problem causes a stack overflow resulting in the system halting for certain commands to the block device. Compaq has determined in laboratory testing that there is a theoretical possibility that during read and write operations to the floppy disk on DS10, DS10L, and ES40 AlphaServers, and VS10 and XP900 AlphaStations, a single byte of data may be inaccurately read or written without notice to the user or system. The potential for this anomaly exists only if floppy data read and write operations are attempted while there is extremely heavy traffic on these Alpha systems' internal input/output busses. Although Compaq has observed the anomaly only in laboratory tests designed to create atypical system stresses, including almost constant use of the floppy disk drive, we are supplying this patch to address this potential issue.

3

Summary of TruCluster Software Patches

This chapter summarizes the TruCluster software patches included in Patch Kit-0008.

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 121.00, 116.00, 118.00, 120.00	New
Patches 1.00, 31.00, 19.00, 24.00, 26.00, 64.00, 76.00, 90.00, 83.00, 98.00, 104.00, 111.00	Superseded by Patch 121.00
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, 91.00, 109.00, 100.00, 103.00, 107.00, 108.00, 112.00, 113.00, 114.00	Superseded by Patch 116.00
Patches 9.00, 17.00, 42.00, 59.00, 61.00, 106.00	Superseded by Patch 120.00

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 This patch 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 This patch 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 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).
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.

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

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 occurred 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 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

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 TruCluster 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. • Fixes a problem where, 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 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 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 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.

- 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.

- Performance improvement in the startup of start scripts. It will reduce the necessary system calls to start the scripts.

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

Patch 95.00 continued	• 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.

Patch 97.00
TCR150-081A
	Patch: Fix SCSI device reservations lost
	
	State: Supersedes patches TCR150-004 (3.00), TCR150-030 (27.00), TCR150-036 (32.00), TCR150-057 (70.00)
	
	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.
	
	• Fixes the following TCR problems:
	
	  – After error events are processed, a timing hole exists whereby important events can be lost.
	
	  – After a HSZ controller failure, SCSI device reservations could get lost because the error events are not being ordered properly.

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

Patch 102.00 TCR150-086	**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), TCR150-074 (86.00), TCR150-085 (101.00)

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 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 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.

- Fixes a problem that can cause a TruCluster member to panic during shutdown.

- Fixes a bug where sometimes a certain shared sequence number will not be freed after use. It also fixes a problem where certain processes could get referenced several times.

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

Patch 105.00 TCR150-089	**Patch:** Shell errors occur if invalid mount option specified **State:** Supersedes patches TCR150-014 (12.00), TCR150-027 (25.00), TCR150-027A-1 (34.01), TCR150-035 (43.00)), TCR150-042 (46.00), TCR150-079 (96.00), TCR150-083 (99.00) 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. • Fixes a problem that would cause an error from awk(1) when modifying an ASE service that contained a large number of LSM volumes. The error would prevent the service from being properly modified. • 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 problem that caused shell errors if an invalid mount option was specified via the asemgr menu.

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

Patch 116.00 TCR150-095	**Patch:** TCR Available Server and Production Server Fixes **State:** New. 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), TCR150-080A (91.00), TCR150-081B (109.00), TCR150-084 (100.00), TCR150-087 (103.00), TCR150-091 (107.00), TCR150-092 (108.00), TCR150-100 (112.00), TCR150-099 (113.00), TCR150-096 (114.00)

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 where, 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.

- 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 116.00 continued	• 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.
	• 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 that 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.
	• Fixes the following TCR problems:
	– After error events are processed, a timing hole exists whereby important events can be lost.
	– After a HSZ controller failure, SCSI device reservations could get lost because the error events are not being ordered properly.
	• Corrects a problem where modifying a service with a large number of DRDs will fail and a "could not malloc" message is seen in the daemon.log.
	• Fixes a problem that caused the asemgr utility to not run when called from a program that is owned by root and has the setuid bit turned on.
	• Corrects a problem in which a network cable failure that corrects within seven seconds of the failure can leave the services in a bad state.
	• Fixes a problem that caused the asemgr to have a memory fault when adding multiple services one after the other.
	• Fixes a problem where timeout values of greater than 30 seconds in /etc/hsm.conf would cause ASE agent to fail at start up.
	• Fixes two issues with clusters:
	– When the clluster is brought up with ASE off, other members report it as UP and RUNNING instead of UP and UNKNOWN.
	– When a restricted service is running on a member, and asemember stop or aseam stop is executed, the service status is still reported as the member name instead of Unassigned.
	• Fixes a problem that caused the asemgr to report that a disk, or mount point, was in multiple services when modifying a service name.
	• Fixes a bug where the aseagent will occasionally core dump on a SCSI bus hang.
Patch 118.00 TCR150-093	**Patch:** mountd exits without error during boot
	State: New
	This patch fixes a problem that could cause mountd to exit without error during boot.

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

Patch 120.00 TCR150-098	**Patch:** Fix for Memory Channel API node crash **State:** New. Supersedes patches TCR150-010 (9.00), TCR150-019 (17.00), TCR150-019B (42.00), TCR150-039B (59.00), TCR150-040B (61.00), TCR150-090 (106.00) 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)

- Fixes a problem that can cause a panic in mcs_wait_cluster_event() when using the Memory Channel API.

- Fixes a problem with the Memory Channel API whereby a node crashes holding an MC-API lock, under certain circumstances the lock will not be released after the node crashes.

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

Patch 121.00 TCR150-097	**Patch:** clumember produces error msg during system startup **State:** New. 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), TCR150-069 (83.00), TCR150-082 (98.00), TCR150-088 (104.00), TCR150-094 (111.00)

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 as follows:

  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.

- Fixes a problem which can cause the following panic:

  panic (cpu 0): rm_update_single_lock_miss: time limit exceeded

- Fixes a problem where /sbin/init.d/clumember produces an error message during system startup if DRD_AUTO_FAILOVER is not defined in /etc/rc.config.

- Fixes a problem that could cause a TruCluster Production server member to hang during boot, and can cause a "simple lock time limit exceeded" panic.

- Fixes a problem that could cause an error to be returned when the Cluster software should wait until a global lock is freed.