Tru64 UNIX 5.1 and TruCluster Server 5.1

Patch Summary and Release Notes for Patch Kit-0004

November 2001

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

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

Compaq Computer Corporation
Houston, Texas

Contents

About This Manual

This manual contains information specific to Patch Kit-0004 for the Tru64™ UNIX 5.1 operating system and TruCluster Server Software™ 5.1 products. It provides a list of the patches contained in each kit and describes the 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 Tru64 UNIX 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 Tru64 UNIX and TruCluster documents:

- Tru64 UNIX and TruCluster *Patch Kit Installation Instructions*
- Tru64 UNIX *Patch Kit Installation Instructions*
- `dupatch`(8) Reference Page
- Tru64 UNIX *Installation Guide*
- TruCluster Server *Cluster Installation*
- TruCluster Server *Cluster Administration*
- Release-specific installation documentation

Reader's Comments

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

You can send your comments in the following ways:

- Fax: 603-884-0120 Attn: UBPG Publications, ZK03-3/Y32
- Internet electronic mail:

  `readers_comment@zk3.dec.com`

  A Reader's Comment form is located on your system in the following location: `/usr/doc/readers_comment.txt`

- Mail:

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

Please include the following information along with your comments:

- The full title of this document.
- The section numbers and page numbers of the information on which you are commenting.
- The version of Tru64 UNIX that you are using.
- If known, the type of processor that is running the Tru64 UNIX software.

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

1

Release Notes

This chapter provides important information that you need in order to work with the Tru64 UNIX 5.1 and TruCluster 5.1 Patch Kit-0004.

1.1 Patch Process Resources

Compaq provides Web sites to help you with the patching process:

- To obtain the lastest patch kit for your operating system and cluster:

  http://ftp1.support.compaq.com/public/unix/

- To view or print the lastest version of the *Patch Kit Installation Instructions* or the *Patch Summary and Release Notes* for a specific patch kit:

  http://www.tru64unix.compaq.com/faqs/publications/patch/

- To visit Compaq's main support page:

  http://www.compaq.com/support/index.shtml

- To visit the Tru64 UNIX homepage:

  http://www.tru64unix.compaq.com/

1.2 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. Compaq recommends that this kit not be placed in the `/`, `/usr`, or `/var` file systems because doing so may unduly constrain the available storage space for the patching activity.

- Permanent Storage Space

  Up to ~80 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 ~82 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 ~958 KB of storage space is required in `/var/adm/patch/doc` for patch abstract and README documentation.

  A total of ~160 KB of storage space is needed in `/usr/sbin/dupatch` for the patch management utility.

TruCluster Server

Note

A rolling upgrade has specific disk space requirements. Be sure to check your disk space before starting a rolling upgrade. Make sure that your system contains the required space in all file systems before you

begin the setup stage of the roll. If any file system fails to meet the minimum space requirements, the program will fail and generate an error message similar to the following:

```
***Error***
The tar commands used to create tagged files in the '/' file system have
reported the following errors and warnings:
NOTE: CFS: File system full: /

        tar: sbin/lsm.d/raid5/volsd : No space left on device
        tar: sbin/lsm.d/raid5/volume : No space left on device
NOTE: CFS: File system full: /

.NOTE: CFS: File system full: /
```

If you receive this message, run the `clu_upgrade -undo setup` command, free up or add the required amount of space on the affected file systems, and then rerun the `clu_upgrade setup` command.

Rolling upgrade disk space requirements are described in Section 7.4.1 of the *TruCluster Server Software Installation* manual.

- Temporary Storage Space

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

- Permanent Storage Space

  Up to ~56 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 ~57 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 ~883 KB of storage space is required in `/var/adm/patch/doc` for patch abstract and README documentation.

  A total of ~168 KB of storage space is needed in `/usr/sbin/dupatch` for the patch management utility.

1.3 Inclusion of Baselevel in tar File Name

With this release, the name of the `tar` file containing the patch distribution has been expanded to include the baselevel for which this kit was built. This formerly internal baselevel number has become a common way of identifying kits. For complete information, see Section 1.3 of the *Patch Kit Installation Instructions*.

1.4 Additional Steps Required When Installing Patches Before Cluster Creation

This note applies only if you install a patch kit before creating a cluster; that is, if you do the following:

1. Install the Tru64 UNIX base kit.
2. Install the TruCluster Server kit.
3. Install the patch kit before running the `clu_create` command.

In this situation, you must then perform three additional steps:

1. Run `versw`, the version switch command, to set the new version identifier:

```
# /usr/sbin/versw -setnew
```

2. Run `versw` to switch to the new version:

```
# /usr/sbin/versw -switch
```

3. Run the `clu_create` command to create your cluster:

```
# /usr/sbin/clu_create
```

1.5 Release Note for KZPCC

Under heavy I/O conditions, an `open()` call to the KZPCC driver can return an I/O error. If this occurs, add the following stanza to your `sysconfigtab` file:

```
I2O:
    Max_Job_Pool_Size=1024
```

In addition, a KZPCC system can hang if you do a physical I/O greater than 4 MB. This is more likely to occur doing I/O to a raw disk with large block size transfers, but can also occur on block devices.

1.6 Release Note for Tru64 UNIX Patch 647.00

1.6.1 Removal of the directio Cloning Patch

This patch provides a script that will allow a user to remove the `directio` cloning patch after the version switch has been thrown by running `clu_upgrade -switch`. This script will set back the version identifiers, request a cluster shutdown, and reboot to finish the deletion of the patch. Another rolling upgrade will be required to delete the patch with `dupatch`.

The `/usr/sbin/clone_versw_undo` script must be run by root in multiuser mode after the `directio` cloning patch has been completely rolled in and before another rolling upgrade has begun. A system or cluster shut down will be required to remove the `directio` cloning patch.

Note

Since the removal of a version switched patch requires a cluster shutdown, only run this script when you are absolutely sure that this patch is the cause of your problem. This script must be run by root in multiuser mode after completing the rolling upgrade that installed the patch and before starting another rolling upgrade. The final removal of the patch can only be accomplished by rebooting the system or cluster after this script completes its processing. This script will offer to shut down your system or cluster at the end of its processing. If you choose to wait, it is your responsiblity to execute the shutdown of the system or cluster.

Do not forget or wait for an extended period of time before shutting down the cluster. Cluster members which attempt to reboot before the entire cluster is shutdown can experience panics or hangs.

See the *Patch Kit Installation Instructions* for further information.

1.6.2 AdvFS and Direct I/O

In laboratory testing, Compaq has observed that under certain circumstances, a possibility exists that inconsistent data may be written to disk on some Tru64 UNIX V5.0A and V5.1 systems running AdvFS and direct I/O.

Compaq became aware of this possibility only during laboratory testing. To our knowledge, no customer has experienced this problem. Compaq is alerting customers to this potential problem as a precautionary measure.

The conditions under which this potential problem may occur are as follows:

- An application writes to a file using AdvFS direct I/O and the file had previously been opened for normal I/O (which by default is cached).
- Some but not all of the pages are still resident in Unified Buffer Cache (UBC) memory.

Invalid data could occur when a single direct I/O write spans multiple AdvFS pages, and some, but not all, of the pages are still in the UBC. If the file has been opened only for direct I/O and remains open for direct I/O, the problem does not exist.

Applications that use direct I/O, such as Oracle, could be affected.

Configurations Affected

The potential problem may affect the following systems:

- Tru64 UNIX V5.0A clustered and nonclustered systems
- Tru64 UNIX V5.1 nonclustered systems only

Only V5.0A and V5.1 systems running an application that uses direct I/O could experience this potential problem. Any application using direct I/O must request this feature explicitly.

The following Oracle versions use direct I/O and may therefore be affected:

- Oracle 8.1.7
- Oracle 8.1.6.3
- Oracle 8.1.6.2 with patch 1527141
- Oracle 8.0.6.2 with patch 1523186
- Oracle 7.3.4.5 with patch 1523179

In addition, the AdvFS file system that is used for any of the following Oracle files:

- Control file
- Data file
- Log file

An Oracle environment meeting the above criteria could experience this potential problem.

Oracle running on raw partitions exclusively or running LSM on raw partitions exclusively are not affected.

Some customers write their own applications that use direct I/O. These customers should be aware of the detailed circumstances under which this problem could occur. The problem could occur as follows:

- The write spans multiple AdvFS 8K pages.
- The last page to be written is in the UBC.
- One or more of the preceding pages are not in the UBC.
- The write to the last page is less than a full page size (8K).

Under these circumstances, the data written at the start of the total write is the original data, offset by the amount of data written to the last page.

Tru64 UNIX versions V4.* and V5.0 are NOT affected.

The potential problem is fixed in future Tru64 UNIX versions and in V5.0 Patch Kit 3 and V5.1 Patch Kit 3.

Problem

If Oracle customers are running one of the affected Oracle configurations, Oracle may have already detected an inconsistency in the database and reported errors similar to the following in the alert log and trace file:

```
ORA-01578: ORACLE data block corrupted (file # 1, block # 100)
ORA-01119: data file 1: '/scratch/820/qa/dbs/t_db1.f'


ORA-00368: checksum error in redo block
ORA-00354: Log corruption near block #231
```

Oracle customers that have run the dbverify (dbv) utility may have encountered an error message similar to the following:

```
***
  Corrupt block relative dba: 0x0040900b (file 0, block 36875)
  Bad header found during dbv:
  Data in bad block -
   type: 27 format: 2 rdba: 0x0040900d
   last change scn: 0x0000.0001349a seq: 0x2 flg: 0x04
   consistency value in tail: 0x349a1b02
   check value in block header: 0xa377, computed block checksum: 0x0
   spare1: 0x0, spare2: 0x0, spare3: 0x0
  ***
```

1.6.3 Technical Update for KZPCC products

This patch provides support for KZPCC products.

For more information see Tru64 UNIX technical updates provided at the following URL:

http://www.tru64unix.compaq.com/faqs/publications/patch/

Select the option for Operating System Technical Updates and choose the following document:

Tru64 UNIX Version 5.1 Technical Update

This technical update will also contain information for valid upgrade paths to Tru64 UNIX Version 5.1 from the Version 4.0x releases that currently support I2O.

1.6.4 Release Note for KZPCC Products

In a TruCluster environment, the deletion and re-creation of any logical drive on a KZPCC controller using the SWCC utility can result in the drive becoming inaccessable. Even though the `hwmgr` sees the drive being deleted and added back, it can not be disklabeled nor can any read/write operation be performed to the drive. Rebooting the system will restore the drive to a usable state.

This will be fixed in the next patch kit.

1.6.5 Problem with Multi-user Mode Application

Warning

When applying this patch in multi-user mode, an inconsistency problem results between the updated `/shlib/libpthread.so` and the existing kernel. The problem manifests itself when you install the patch in multi-user mode and you elect to reboot at a later time. The scheduled reboot will not occur. This problem can be avoided by installing Patch

647.00 in single user mode, or selecting the option to reboot now (rather than scheduling later).

To correct this situation, if you have installed the patch and have not rebooted the system, execute the following commands:

1. Set DUPATCH_SESLOG to location of session log, by default:

   /var/adm/patch/log/session.log

2. Get the name of newly-built kernel:

   # **NEW_KERNEL=‘grep "The new kernel is" $DUPATCH_SESLOG | awk ’ { print $5 }’ ‘**

3. Copy the new kernel:

   # **cp <NEW_KERNEL> /vmunix**

4. Reboot the system at a specified time:

   # **shutdown -r <TIME_OF_REBOOT>**

After rebooting with the new kernel, your system will once again be consistent.

1.6.6 New Graphics Card

This patch provides the driver support for a new graphics card. In order to obtain full support for this graphics card, you must also select Patch 509.00, which is the X server portion of the patch.

A list of supported platforms is available on the following web page:

http://www.compaq.com/alphaserver/products/options.html

If you have a system with this new 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 new graphics card.

---

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

6. Shut down the system:

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

7. Boot the new kernel:

   >>> **boot**

If you remove this patch from your system after you have rebuilt the kernel to incorporate support for the new 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 new graphics card and will include generic VGA graphics support in the resulting kernel.

1.6.7 DEGPA-TA Gigabit Ethernet Device

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

To do this, follow these steps:

1. Shut down the system:

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

2. Boot `genvmunix` to single-user mode:

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

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

   # **/sbin/bcheckrc**

   # **/sbin/update**

   # **/sbin/swapon -a**

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

   # **/usr/sbin/doconfig**

   Note

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

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

6. Shut down the system:

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

7. Boot the new kernel:

   >>> **boot**

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

1.6.8 Configuring FibreChannel Systems

This patch requires that FibreChannel systems which utilize FibreChannel devices for boot and swap be properly configured as follows:

- There is a minimum of 1.25 -2 times physical memory for swap space available.
- All boot and swap devices are properly configured to use one of the four console ports.
- The console WWID number for each boot or swap device is identical to the WWID number found via the hwmgr utility using the steps outlined as follows:

  1. Identify the console port(N) and WWID number configuration information using consvar as follows:

     ```
     consvar -g N1 ; consvar -g N2
     consvar -g N3 ; consvar -g N4
     consvar -g wwid0 ; consvar -g wwid1
     consvar -g wwid2 ; consvar -g wwid3
     ```

  2. Find the device name by checking `etc/fstab`, using `showfdmn` for AdvFS root domains, and `swapon -s` for swap devices for each FibreChannel boot and swap device.
  3. Find the HWID using the device name obtained in step 2

     `hwmgr -view dev | grep "device name from step 2 above"`

     for each FibreChannel boot and swap device.
  4. Find the WWID using the device name obtained in step 3

     `hwmgr -view dev | grep "device name from step 3 above"`

     for each FibreChannel boot and swap device.
  5. Verify that the hwmgr WWIDs from step 4 above match the WWIDs from step 1 above for each FibreChannel boot and swap device.
  6. If the WWIDs do not match in step 5 then the system needs to be shut down and reconfigured using the wwidmgr utility as described in the Wwidmgr Users Manual located in the doc directory on the Firmware CDROM until you have verified that the WWID console configuration matches the system hwmgr WWID configuration using the steps described previously.

1.7 Release Note for Tru64 UNIX Patches 324.00 and 496.00

This patch delivers version V1.0-032 of the `libots3` library. Version 2.0 (or greater) of the `libots3` library is delivered with the Compaq FORTRAN Compiler, Versions V5.3 ECO1 and V5.4, or the Developers Tool Kit (DTK) (OTABASE subset). If `libots3` V2.0 (or greater) is already installed on your system, and you install this patch, you will receive the following informational message:

```
Problem installing:


- Tru64_UNIX_V5.1 / Software Development Environment Patches:

      Patch 00496.00 - Fix for problems in Compaq C compiler


       ./usr/shlib/libots3.so:

                 is installed by:

                                OTABASE212
               and can not be replaced by this patch.

This patch will not be installed.
```

To determine what version of `libots3` library is installed on your system, execute the following command:

```
# what /usr/shlib/libots3.so libots3.so:
libots3.a       V2.0-094 GEM 27 Feb 2001
```

1.8 Release Note for Tru64 UNIX Patch 614.00

This release note contains a new reference phge for the `fixfdmn` utility.

NAME
fixfdmn - Checks and repairs corrupted AdvFS domains

SYNOPSIS

/sbin/advfs/fixfdmn [-mtype[,type]...] [-d directory] [-v number] [-a [-c] | -n] [-s {y | n}] [domain] [fileset]

/sbin/advfs/fixfdmn -u directory domain

OPTIONS

-a Specifies that after repairing what it can, fixfdmn will attempt to activate the domain at the end of the run. This option cannot be used with the -n option.

-c Removes any clone filesets. This option is only valid if used with the -a option.

-d directory
Specifies a directory to which the message log and undo files will be written. If the -d option is not used, the message and undo log files are put in the current working directory. The message log file is named fixfdmn.<domain>.log and the two undo files are named undo.<domain>.<#> and undoidx.<domain>.<#> where # will cause a number to be appended to the filenames to make them unique. The numbers will be rotated sequentially from 0 (zero) through 9 if multiple undo files are created for the same domain. The undo file will have the same ending number as its corresponding undo index file.

-m type[,type...]
Specifies a list of types of metadata, one or more of which can be checked and repaired. The valid types are log, sbm, sync, bmt, frag, quota and files. If you specify the fileset parameter, sync, log, sbm, and bmt are made invalid types for the -m option. If you do not specify -m, the default is to check all types.

sync
Corrects the magic number and synchronizes data across volumes (for example, volume numbers, mount ids, mount states, domain ids, and so on.)

log Resets the transaction log so it is not processed.

sbm Synchronizes the sbm to the information in the bmt.

bmt Corrects the bmt.

frag
Corrects frag file groups and free lists and ensures that all file frags reside in the frag file.

quota
Checks and corrects sizes of quota files.

files
Verifies that directory metadata is correct.

-n Specifies that fixfdmn will check the domain and not do any repairs. It will report what problems were found and how it would have fixed them.

-s {y | n}
Specifies that "yes" or "no" should be answered to prompts when run from a script.

-u directory
Restores the domain to its previous state by undoing the effects of the last run of fixfdmn, using the most recent undo files in the specified directory.

-v number
Specifies the verbose mode level which controls the messages printed to stdout.

0 = Only error messages

1 = (Default) Progress, errors and summary messages

2 = Progress messages, detailed error messages, fix information and summary messages

OPERANDS

domain
The name of a corrupted domain to repair.

fileset
The name of the fileset to repair if only one fileset in this domain exhibits errors. You may tell fixfdmn to check only that fileset and not specifically look for errors in other filesets.

DESCRIPTION

The fixfdmn utility checks and repairs corrupt AdvFS domains and filesets.

The fixfdmn utility is primarily concerned with fixing problems that have a limited scope. When a large portion of the domain is corrupted, there is very little fixfdmn can do, so it will recommend restoring data from backup or running the salvage(8) command.

The fixfdmn utility uses the on-disk metadata to determine what corruptions exist in the domain. Only metadata will be repaired, as there is currently no way to check or repair the contents of users files. Only those problems which prevent mounting the domain, or would result in a domain or system panic, will be repaired.

After major areas of metadata are checked, and if a corruption was fixed, fixfdmn will prompt the user to determine if they want to continue looking for additional corruption.

If fixfdmn detects an error in a clone fileset, the clone is marked out of sync and should not be used.

If fixfdmn cannot recover the metadata for a specific file, the file may be truncated, moved, or deleted depending on the situation. The fixfdmn utility will attempt to save as much of a file as possible.

Every page fixfdmn changes will be saved to an undo file. If the user does not like the results of running fixfdmn, the user can undo the changes by running fixfdmn again with the -u option. If the file system containing the undo files runs out of space during the fixfdmn run, the user will be prompted on how to proceed. The user will have the option to continue without the undo files, to continue adding more space to the domain containing the undo files, or to exit.

Use the -m type option when you have information from a system/domain panic or output from verify or other tools which indicate where the corruption may be. This option limits the scope of what is checked and repaired.

NOTES

The fixfdmn command will always clear the transaction log, even on a non-corrupt domain unless the -n option is specified

There must be a domain entry for this domain in /etc/fdmns. The fixfdmn command opens the block devices specified for the volumes in /etc/fdmns.

If you need to repair the root domain, you must boot from CD-ROM and create the entry for the root domain under /etc/fdmns.

RESTRICTIONS

You must be root to run fixfdmn.

The fixfdmn command requires that the domain specified will have no filesets mounted.

Although fixfdmn may report success, it does not guarantee that all corruptions have been eliminated.

If a domain is mounted and written to after being repaired by fixfdmn, using the fixfdmnutility with the -u option will likely cause corruptions.

EXIT STATUS

0 (Zero)
Success.

1 Corrupt
Unable to repair all found corruptions

2 Failure
Program or system error

FILES

/etc/fdmns
Contains AdvFS domain directories and locks.

SEE ALSO

Commands: salvage(8), umount(8), verify(8), vrestore(8)

1.9 Release Note for Tru64 UNIX Patch 509.00

This patch provides the X server support for a new graphics card. In order to obtain full support for this graphic card, you must also select Patch 647.00, which is the driver portion of the patch.

A list of supported platforms is available on the following web page:

http://www.compaq.com/alphaserver/products/options.html

1.10 Release Note for Tru64 UNIX Patch 391.00

This patch contains a solution for the following issue:

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

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

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

The solution to this issue is also available as an individual, manually installed patch kit named `floppy_CSP_v51.tar.gz`, available from:

`http://ftp1.support.compaq.com/public/unix/v5.1`

1.11 Release Note for TruCluster Patch 82.00

This patch fixes a problem that can occur when an application does a direct I/O write (an AdvFS file was opened with the O_DIRECTIO flag) or when an application performs asynchronous Direct I/Os to files using the `aio_raw` library, and the target file resides on a fileset that has been cloned.

This patch uses the rolling upgrade version switch to ensure that all members of the cluster have installed the patch before it is enabled.

Prior to throwing the version switch, you can remove this patch by returning to the rolling upgrade install stage, rerunning `dupatch`, and selecting the Patch Deletion item in the Main Menu.

You can remove this patch after the version switch is thrown, but this requires a shutdown of the entire cluster.

To remove this patch after the version switch is thrown, use the following procedure:

Note:

Use this procedure only under the following conditions:

- The rolling upgrade that installed this patch, ncluding the clean stage, has completed.
- The version switch has been thrown (clu_upgrade -switch).
- A new rolling upgrade is not in progress.
- All cluster members are up and in multi-user mode.

1. Run the `/usr/sbin/clone_versw_undo` command.

   When this command completes, it asks whether it should shut down the entire cluster now. The patch removal process is not complete until after the cluster has been shut down and restarted.

   If you do not shut down the cluster at this time, you will not be able to shut down and reboot an individual member until the entire cluster has been shut down.
2. After cluster shutdown, boot the cluster to multi-user mode.
3. Rerun the rolling upgrade procedure from the beginning (starting with the setup stage). When you rerun dupatch, select the Patch Deletion item in the Main Menu.

For more information about rolling upgrades and removing patches, see the Patch Kit Installation Instructions.

1.12 Release Note for TruCluster Server Software

During the switch stage of a rolling upgrade from TruCluster Server Version 5.1 to TruCluster 5.1 Patch Kit-0003, you may see the following message:

```
Initiating version switch on cluster members
.Switch already switched
```

You can safely ignore this message. The switch stage will complete successfully.

1.13 Release Note for Misleading Error Messages

The release note explains misleading error messages you may see while deleting patches in a cluster.

There is a bug in the current version of the patch tools where messages similar to the following may be observed:

```
- Tru64_UNIX_V5.1A / X11 Patches:
        Patch 00057.00 - Fix for X server
hang

can only be deleted by using the Tru64 UNIX Patch Utility
(/usr/sbin/dupatch).
------------------------------------------------------------------------
setld: OSFPAT00005700520 scp failed on member63.
```

These messages are misleading and can be ignored since they originate while running the Tru64 UNIX dupatch Utility tool.

1.14 Release Note for Broken Link Problem

When performing a baseline analysis with the dupatch utility on Tru64 UNIX 5.1 systems, the baseline error log files may report that a number of files have broken hard links to the /usr/share/man/man3 directory.

The presence of these broken links will not affect your system operation, the installation of dupatch or dupatch tools, the successful installation of patches, or the rebuilding of kernels on the system. The problem will be addressed in a future version of the operating system.

You can determine if these broken links exist on your system by performing the following steps:

1. Change directories as follows:

   # **cd /usr/share/man/man3**

2. Check to see that the inodes are the same for all the files:

   # **ls -il slk*.3.gz curs_slk.3.gz**

An example of a correct hard link would look as follows. Note the same inodes.

```
14648 -rw-r--r--  17 root     system      2086 Mar  9  2000 curs_slk.3.gz
14648 -rw-r--r--  17 root     system      2086 Mar  9  2000 slk_attr_off.3.gz
14648 -rw-r--r--  17 root     system      2086 Mar  9  2000 slk_attr_on.3.gz
14648 -rw-r--r--  17 root     system      2086 Mar  9  2000 slk_attr_set.3.gz
14648 -rw-r--r--  17 root     system      2086 Mar  9  2000 slk_attroff.3.gz
14648 -rw-r--r--  17 root     system      2086 Mar  9  2000 slk_attron.3.gz
14648 -rw-r--r--  17 root     system      2086 Mar  9  2000 slk_attrset.3.gz
14648 -rw-r--r--  17 root     system      2086 Mar  9  2000 slk_clear.3.gz
14648 -rw-r--r--  17 root     system      2086 Mar  9  2000 slk_color.3.gz
14648 -rw-r--r--  17 root     system      2086 Mar  9  2000 slk_init.3.gz
14648 -rw-r--r--  17 root     system      2086 Mar  9  2000 slk_label.3.gz
14648 -rw-r--r--  17 root     system      2086 Mar  9  2000 slk_noutrefresh.3.gz
14648 -rw-r--r--  17 root     system      2086 Mar  9  2000 slk_refresh.3.gz
14648 -rw-r--r--  17 root     system      2086 Mar  9  2000 slk_restore.3.gz
14648 -rw-r--r--  17 root     system      2086 Mar  9  2000 slk_set.3.gz
14648 -rw-r--r--  17 root     system      2086 Mar  9  2000 slk_touch.3.gz
14648 -rw-r--r--  17 root     system      2086 Mar  9  2000 slk_wset.3.gz
```

An example of an incorrect hardlink would look as follows. Note the different inodes.

```
54891 -rw-r--r--   2 root     system      2086 Aug 11 17:32 curs_slk.3.gz
54891 -rw-r--r--   2 root     system      2086 Aug 11 17:32 slk_attr_off.3.gz
55583 -rw-r--r--  15 root     system      2086 Aug 11 17:32 slk_attr_on.3.gz
55583 -rw-r--r--  15 root     system      2086 Aug 11 17:32 slk_attr_set.3.gz
55583 -rw-r--r--  15 root     system      2086 Aug 11 17:32 slk_attroff.3.gz
55583 -rw-r--r--  15 root     system      2086 Aug 11 17:32 slk_attron.3.gz
55583 -rw-r--r--  15 root     system      2086 Aug 11 17:32 slk_attrset.3.gz
55583 -rw-r--r--  15 root     system      2086 Aug 11 17:32 slk_clear.3.gz
```

```
55583 -rw-r--r--  15 root     system      2086 Aug 11 17:32 slk_color.3.gz
55583 -rw-r--r--  15 root     system      2086 Aug 11 17:32 slk_init.3.gz
55583 -rw-r--r--  15 root     system      2086 Aug 11 17:32 slk_label.3.gz
55583 -rw-r--r--  15 root     system      2086 Aug 11 17:32 slk_noutrefresh.3.gz
55583 -rw-r--r--  15 root     system      2086 Aug 11 17:32 slk_refresh.3.gz
55583 -rw-r--r--  15 root     system      2086 Aug 11 17:32 slk_restore.3.gz
55583 -rw-r--r--  15 root     system      2086 Aug 11 17:32  slk_set.3.gz
55583 -rw-r--r--  15 root     system      2086 Aug 11 17:32 slk_touch.3.gz
55583 -rw-r--r--  15 root     system      2086 Aug 11 17:32 slk_wset.3.gz
```

1.15 Release Note for Potential Rolling Upgrade Problem

When patching a clustered Tru64 UNIX 5.1 system using the rolling upgrade procedure, the operation may fail if your system has been upgraded from a patched Tru64 UNIX 5.0A version.

In such cases, the lead member is successfully patched, but the patching operation fails for subsequent members. The problem occurs because the file `var/adm/patch/roll/installed_patches` contains the old `OSFPAT*505` entries, which no longer exist in `./usr/.smdb`. As a result, the rolling upgrade generates error messages such as the following when subsequent members are rolled:

```
Backing up member-specific data for member: 2
 .......
 grep: can't open ./usr/.smdb./OSFPAT00018600505.inv
 grep: can't open ./usr/.smdb./OSFPAT00019200505.inv
 grep: can't open ./usr/.smdb./OSFPAT00020500505.inv
 grep: can't open ./usr/.smdb./OSFPAT00021100505.inv
 grep: can't open ./usr/.smdb./OSFPAT00016500505.inv
 grep: can't open ./usr/.smdb./OSFPAT00020000505.inv
```

The following procedures describe how to solve the problem if you discover it during a rolling upgrade or if you have not yet begun the rolling upgrade.

Rolling Upgrade Started

Perform the following steps if you issued the `clu_upgrade` command and discovered the error during the roll of the second member (designated here as member 2):

1. Halt the failing member:

   # **halt**

2. On the lead member, undo the roll:

   # **clu_upgrade undo roll 2**

3. Remove the old `OSFPAT*505` entries from `/var/adm/patch/roll/installed_patches`. Because this is a cluster-common file, you need only do this once. The remaining members can be rolled as documented in the *Patch Kit Installation Instructions*.

   a. Change to the `/var/adm/patch/roll` directory:

      # **cd /var/adm/patch/roll**

   b. Invoke an editor such as `vi` and remove any lines that contain the string `OSFPAT*505` from the file `installed_patches`:

      # **vi ./installed_patches**

4. Boot member 2 to multiuser mode and then shut down to single-user mode:

   >>> **boot**

   # **shutdown now**

5. Roll member 2:

   ```
   # bckeckrc

   # clu_upgrade roll
   ```

6. Complete the procedure as documented in the *Patch Kit Installation Instructions*.

Rolling Upgrade Not Started

Perform the following steps if you have not started a rolling upgrade:

1. Rename the `installed_patches` file and re-create it.

   ```
   # cd /var/adm/patch/roll/
   # mv ./installed_patches ./installed_patches.V50A
   # touch ./installed_patches
   ```

2. Complete the procedure as documented in the *Patch Kit Installation Instructions*.

For information on patching your clustered system using the rolling upgrade procedure, see the *Patch Kit Installation Instructions* and the `clu_upgrade`(8) reference page.

1.16 Release Note for Tru64 UNIX Patch 169.00

In cases where the `bttape` or `btcreate` command is used to back up and restore UFS file systems, `btextract` leaves behind a `symboltable` file in the restored file system. This file, if present, will cause `btextract` to hang the next time a bootable tape is created using `btcreate` or `bttape`. The `btextract` command hangs while trying to restore the UFS file system.

To work around this problem, ensure that the file `restoresymtab?` (where ? refers to the cluster member ID, 0 by default) is removed. Every UFS file system that was restored using `btextract` will have this file, and this file needs to be removed on each file system before running the `bttape` or `btcreate` command the next time. For example, if `/` and `/usr` are backed up, then the file will be found at `/restoresymtable0` and `/usr/restoresymtable0`, and both instances of the file need to be removed before proceeding with `btcreate` or `bttape`.

1.17 Release Note for Tru64 UNIX Patch 270.00

This patch fixes a security vulnerability (called the Brown Orifice) in Netscape Communicator Version 4.72 by updating Netscape Communicator to Version 4.75.

To determine which version of Netscape Communicator you are running, click on the Help button in the toolbar at the top of the Navigator component window, then choose the About Communicator option from the drop down menu.

You can download the latest version of Netscape Communicator for Tru64 UNIX from the Netscape Download World Wide Web site:

`http://home.netscape.com/download/index.html`

Or, from the Compaq Tru64 UNIX World Wide Web site:

`http://www.tru64unix.compaq.com/internet/download.htm`

If you are unable to upgrade to Netscape Communicator 4.75 or later, you can avoid this security vulnerability by disabling the browser's ability to run Java by following these steps:

1. Start Netscape Communicator:

   $**/usr/bin/X11/netscape**

2. Click on the Edit button in the toolbar at the top of the Navigator component window.
3. Click on the Preferences... option on the drop down menu that appears when the Edit button is selected. This displays the Netscape: Preferences dialog box.
4. In the window pane on the left of the Netscape: Preferences dialog box, click on the Advanced tab. This displays the advanced Communicator preferences in the dialog box.
5. If the box next to the Enable Java preference has a check mark in it, click on the box to remove the check mark. This will disable the Java programming language. Then, click on the Okay button in the Advanced preferences dialog box. (If there is no check mark in the box, you do not need to take any action.)
6. Exit Netscape Communicator by clicking on the Exit option in the drop down menu that appears when you click on the File button on the toolbar at the top of the Navigator window.

Disabling Java ensures Netscape Communicator is not vulnerable to the Brown Orifice vulnerability. You do not have to disable JavaScript.

Note

If you use the Japanese or Chinese interfaces provided in the Worldwide Language Support software, you must update the Communicator version numbers in the `/usr/lib/X11/*/app-defaults/Netscape` file if you choose to upgrade to Netscape Communicator Version 4.75 or later.

If the version numbers in these files do not match the version of Netscape Communicator installed, it will not run in the Japanese or Chinese locales.

You can download the updated files from the Compaq Tru64 UNIX World Wide Web site:

http://www.tru64unix.compaq.com/internet/download.htm

2

Summary of Base Operating System Patches

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

Table 2–1 lists patches that have been updated.

Table 2–2 provides a summary of patches.

Table 2–1: Updated Base Operating System Patches

Patch IDs	Change Summary
Patches 494.00, 498.00, 500.00, 513.00, 515.00, 517.00, 519.00, 523.00, 525.00, 546.00, 550.00, 554.00, 556.00, 558.00, 561.00, 569.00, 571.00, 573.00, 575.0, 577.00, 579.00, 581.00, 585.00, 587.00, 589.00, 593.00, 595.00, 598.00, 600.00, 602.00, 607.00, 609.00, 614.00, 620.00, 622.00, 628.00, 632.00, 647.00, 649.00	New
Patches 13.00, 175.00, 406.00	Superseded by Patch 408.00
Patches 66.00, 322.00	Superseded by Patch 496.00
Patches 1.00, 2.00, 3.00, 5.00, 87.00, 88.00, 90.00, 233.00, 234.00, 235.00, 236.00, 237.00, 238.00, 239.00, 124.00, 241.00, 243.00, 501.00, 502.00	Superseded by Patch 504.00
Patches 246.00, 247.00, 249.00, 119.00, 287.00, 505.00, 506.00, 507.00	Superseded by Patch 509.00
Patches 64.00, 256.00, 257.00, 258.00, 260.00	Superseded by Patch 521.00
Patches 308.00, 55.00, 266.00, 268.00, 526.00	Superseded by Patch 528.00
Patch 401.00	Superseded by Patch 530.00
Patch 405.00	Superseded by Patch 532.00
Patch 403.00	Superseded by Patch 534.00
Patch 278.00	Superseded by Patch 536.00
Patches 288.00, 290.00	Superseded by Patch 538.00
Patch 292.00	Superseded by Patch 540.00
Patches 128.00, 288.00, 541.00	Superseded by Patch 543.00
Patch 300.00	Superseded by Patch 548.00
Patch 134.00	Superseded by Patch 552.00
Patch 68.00	Superseded by Patch 563.00
Patch 316.00	Superseded by Patch 565.00
Patch 31.00	Superseded by Patch 567.00
Patch 21.00	Superseded by Patch 583.00
Patch 57.00	Superseded by Patch 591.00
Patch 596.00	Superseded by Patch 598.00
Patches 72.00, 354.00, 355.00, 356.00, 358.00, 603.00	Superseded by Patch 605.00
Patches 126.00, 610.00	Superseded by Patch 612.00
Patches 135.00, 137.00	Superseded by Patch 616.00

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

Patches 138.00, 140.00	Superseded by Patch 618.00
Patches 145.00, 146.00, 148.00, 370.00	Superseded by Patch 624.00
Patch 376.00	Superseded by Patch 626.00
Patch 378.00	Superseded by Patch 630.00
Patches 331.00, 333.00, 511.00	Superseded by Patch 634.00
Patch 389.00	Superseded by Patch 636.00
Patch 395.00	Superseded by Patch 638.00
Patches 250.00, 252.00, 59.00, 156.00, 53.00, 60.00, 62.00, 151.00, 152.00, 154.00, 11.00, 22.00, 23.00, 24.00, 25.00, 26.00, 27.00, 28.00, 29.00, 30.00, 32.00, 86.00, 93.00, 94.00, 95.00, 96.00, 97.00, 98.00, 99.00, 100.00, 101.00, 103.00, 163.00, 165.00, 167.00, 176.00, 177.00, 178.00, 179.00, 180.00, 181.00, 182.00, 183.00, 184.00, 185.00, 186.00, 187.00, 188.00, 189.00, 190.00, 191.00, 192.00, 193.00, 194.00, 195.00, 196.00, 197.00, 198.00, 199.00, 200.00, 201.00, 202.00, 203.00, 204.00, 205.00, 206.00, 207.00, 208.00, 209.00, 210.00, 211.00, 212.00, 213.00, 214.00, 215.00, 216.00, 217.00, 218.00, 219.00, 220.00, 221.00, 222.00, 224.00, 399.00, 328.00, 92.00, 366.00, 409.00, 410.00, 411.00, 412.00, 413.00, 414.00, 415.00, 416.00, 417.00, 418.00, 419.00, 420.00, 421.00, 422.00, 423.00, 424.00, 425.00, 426.00, 427.00, 428.00, 429.00, 430.00, 431.00, 432.00, 433.00, 434.00, 435.00, 436.00, 437.00, 438.00, 439.00, 440.00, 441.00, 442.00, 443.00, 444.00, 445.00, 446.00) 447.00, 448.00, 449.00, 450.00, 451.00) 452.00, 453.00, 454.00, 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, 479.00, 480.00, 481.00, 482.00, 483.00, 484.00, 485.00, 486.00, 487.00, 488.00, 489.00, 490.00, 492.00, 639.00, 640.00, 641.00, 642.00, 644.00, 645.00	Superseded by Patch 647.00

Table 2–2: Summary of Base Operating System Patches

Patch IDs	Abstract
Patch 7.00 OSF510-037B	**Patch:** Threaded programs do not terminate **State:** Existing This patch fixes hangs in threaded programs with subprocesses created with nfork(NULL). Examining one of the hanging subprocesses shows that it has called fopen() and is waiting for the iobptr mutex in _findiop().
Patch 15.00 OSF510-009A	**Patch:** libst shared library fix **State:** Existing This patch fixes a problem with two routines in the libst library, st_obj_open() and st_obj_write(). The ability to change a file permission using these two libst routines is denied if a group has write permissions.
Patch 17.00 OSF510-009B	**Patch:** libst static library fix **State:** Existing This patch fixes a problem with two routines in the libst library, st_obj_open() and st_obj_write(). The ability to change a file permission using these two libst routines is denied if a group has write permissions.
Patch 19.00 OSF510-036	**Patch:** Fix for booting problem via network interface **State:** Existing This patch solves a problem which could prevent a V5.1 kernel from booting via a network interface. It corrects a timing issue which affects processors with speeds in excess of 700MHz.
Patch 38.00 OSF510-021	**Patch:** Fix for panic that occurs when kloadsrv is restarted **State:** Existing This patch fixes a system panic that may occur when /sbin/kloadsrv is restarted.
Patch 40.00 OSF510X11-001	**Patch:** Fix for lbxproxy utility **State:** Existing This patch fixes a problem where the X windows lbxproxy utility, which is used to make Low Bandwidth X (LBX) connections to an X server, did not accept local connections.
Patch 49.00 OSF510-024	**Patch:** Fixes the processing of export lists **State:** Existing This patch fixes the processing of export lists with a / (slash) in them.
Patch 51.00 OSF510-043	**Patch:** Change to kloadsrv and hotswapd entries **State:** Existing This patch changes the kloadsrv and hotswapd entries in the /etc/inittab file. The change will prevent possible problems with dynamically loaded kernel modules when shutting down to single user mode.
Patch 74.00 OSF510-018	**Patch:** Fixes environmental warning in GS systems **State:** Existing This patch fixes a problem on the AlphaServer GS80, GS160, and GS320 platforms where the system will issue an environmental warning and shut itself down when it reaches a critical temperature, even though this temperature is safe for the power supply.
Patch 76.00 OSF510-038	**Patch:** Hardware manager inaccurately reports the CPU speed **State:** Existing This patch fixes a problem where the hardware manager inaccurately reports the CPU speed. It reported a CPU speed that was one MHz less than the correct speed.

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

Patch 82.00 OSF510CDE-001	**Patch:** List of application groups is not re-created **State:** Existing This patch fixes a problem where the Common Desktop Environment (CDE) Application Manager did not re-create the list of application groups at login. After customizing the application groups, users would see the old groups instead of the new groups.
Patch 105.00 OSF510-017	**Patch:** Prevents not currently mounted warning messages **State:** New This patch prevents "not currently mounted" warning messages from being displayed for file systems the user did not request to umount.
Patch 107.00 OSF510X11-007	**Patch:** Fix for tcl **State:** New This patch fixes a problem in which tclhelp and any other tool using #!/usr/bin/wishx as the interpreter fails when additional versions of tcl are installed in /usr/local.
Patch 109.00 OSF510-085	**Patch:** btextract does not create device special files **State:** New. Supersedes patches OSF510-045 (45.00), OSF510-029 (47.00) This patch corrects the following: • Adjusts the sleep time for slower robot tape changers to allow them time to replace a tape. • Fixes a kernel panic caused by btcreate when it generated scripts to recreate LSM volumes on restore operations. • Fixes a problem where the device special files are not being created by btextract.
Patch 111.00 OSF510DX-003	**Patch:** Fix for smsd crash **State:** New This patch fixes intermittent crashes of the SysMan Station daemon (smsd) that are most likely to occur at system startup time, midnight, or during reconfiguration of system components. This crash would render a connected SysMan Station client unusable.
Patch 114.00 OSF510X11-009A	**Patch:** Fix for Xt **State:** New. Supersedes patch OSF510X11-005A (112.00) This patch corrects the following: • Fixes a memory leak in the X Window System's X Toolkit library (Xt) that could occur when creating and destroying Motif List, Text, and TextField widgets. • Fixes the problem of XmStringGetLtoR() failing in dxhanziim when it runs in a C/en_US.ISO8859-1 locale.
Patch 117.00 OSF510X11-009B	**Patch:** Fixes a memory leak in Xt **State:** New. Supersedes patch OSF510X11-005B (115.00) This patch corrects the following: • Fixes a memory leak in the X Window System's X Toolkit library (Xt) that could occur when creating and destroying Motif List, Text, and TextField widgets. • Fixes the problem of XmStringGetLtoR() failing in dxhanziim when it runs in a C/en_US.ISO8859-1 locale.

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

Patch 121.00 OSF510CDE-002	**Patch:** Fix for dtlogin **State:** New This patch 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.
Patch 124.00 OSF510DX-006	**Patch:** Message fragments now I18N compatible **State:** Supersedes patches OSF510DX-002 (36.00), OSF510DX-005 (122.00) This patch fixes the following dxaccounts problems: • A system running ASU experiences a dxaccounts crash problem when a user is deleted from PC User view. • The dxaccounts dialog messages are incorrectly displayed when a user is added with no password entry. • The dxaccounts utitlity is unable to create a new user from the PC Users view on a system with ASU installed. • The following problems can occur with the dxaccounts application on ASU system: – The dxaccounts utility crashes when the root icon is double clicked. – The full name of a new PC account is not mapped to a UNIX user. – Erasing a PC account's fields does not work; the values erased remain. – The default values of Home Directory, Login Script, and User Profile Path for a PC user are invalid. • Changing root's login/uid is enabled via cli/dxaccounts utilities. • Incorrect results of usermod -G. • The -x account_inactive | account_expiration options do not set the attributes. • 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. • Fixes message fragments to make them I18N compatible.
Patch 130.00 OSF510-067	**Patch:** Fix for lock hierarchy violation panic **State:** New. Supersedes patch OSF510-034 (80.00) This patch corrects the following: • Fixes a problem that can occur under certain circumstances with an IPv6 packet that contains a routing header. This could possibly crash a machine functioning as an IPv6 router. This was only reproduced with manually generated packets. • Under certain circumstances a Tru64 UNIX system configured with IPv6 can panic with a lock hierarchy violation. This panic can occur on any system running Tru64 UNIX with IPv6 enabled and configured.
Patch 142.00 OSF510X11-006A	**Patch:** Fixes memory leaks in Motif library **State:** New This patch fixes various memory leaks in the Motif library (libXm) that could occur when creating and destroying Motif List, Text, and TextField widgets.

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

Patch 144.00 OSF510X11-006B	**Patch:** Fix for libXm **State:** New This patch fixes various memory leaks in the Motif library (libXm) that could occur when creating and destroying Motif List, Text, and TextField widgets.
Patch 150.00 OSF510-052	**Patch:** Fix for advscan **State:** New This patch fixes a problem where advscan -a -g does not display bootable partitions properly.
Patch 158.00 OSF510CDE-003	**Patch:** Fix for dtmail problem **State:** New This patch fixes a dtmail problem in which a From line with quotes in it incorrectly finds the date of the mail message. This error is displayed on the main screen under the header Date and Time and shows up as Dec. 31 or as a blank field.
Patch 162.00 OSF510DX-004	**Patch:** Fix for diskconfig error message **State:** New This fixes a problem that was causing diskconfig to issue the error message "can't read tminor: no such variable" upon startup.
Patch 169.00 OSF510DX-009	**Patch:** Fix for bttape **State:** New bttape now uses the lock file /usr/run/bttape.pid for checking multiple instances. Also, the default addlist and fslist are created appropriately.
Patch 171.00 OSF510-098	**Patch:** Fix for voldctl stop command **State:** New This patch corrects the voldctl stop command behaviour for cluster support.
Patch 173.00 OSF510-057	**Patch:** fixso command causes segmentation fault **State:** New This patch fixes a problem with the /usr/ucb/fixso command that can cause a segmentation fault.
Patch 226.00 OSF510-107B	**Patch:** Fix for delayed AdvFS requests **State:** New This patch corrects some I/O rate fluctuations and thread unresponsiveness that had been seen when vm free pages dropped to a low level and used pages were being recycled.

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

Patch 230.00 OSF510-109B	**Patch:** Fix for POSIX Threads Library **State:** Supersedes patches OSF510-039B (34.00), OSF510-212B (227.00), OSF510-206B (228.00) This patch fixes problems for threaded applications running on Tru64 UNIX V5.1: • Fixes a bug in the POSIX Threads Library for Tru64 UNIX V5.1 where a terminating thread did not properly clear an enabled floating point unit, causing invalid floating point state on the next thread that is run. • Fixes a bug in the POSIX Threads Library for Tru64 UNIX V5.1 that would result in a DECthreads error return of EINVAL from the pthread mutex API routines. This error would be seen only when the thread stack had been user defined/changed, specifically seen when using the user level context switching (ucontext) routines. • Fixes a bug in the POSIX Threads Library for Tru64 UNIX V5.1 that would result in a DECthreads Bugcheck and process termination. Threaded applications might encounter this problem when pthread_kill() is used on a thread that is marked as blocked in the kernel.
Patch 232.00 OSF510-158B	**Patch:** Adds support for activating temporary data logging **State:** New This patch provides support for activating temporary data logging on a mount point.
Patch 245.00 OSF510-198	**Patch:** Install does not allow subset name with an underscore **State:** New. Supersedes patch OSF510-046 (9.00) This patch fixes the following problems: • Fixes a problem with the installation process rejecting a subset name with an underscore character on a V5.1 system. Specifically, when a user was trying to install the IBM MQSeries Documentation Base subset, MQS_HTML_PUBS. • Fixes a problem with the deletion process on a cluster system when a member node is running /usr/bin/csh. The process fails with a command not found error. • Fixes a problem with the deletion process not terminating when the C DELETE phase of the subset control program fails.
Patch 255.00 OSF510-090	**Patch:** tar -F ignores files named err **State:** New. Supersedes patch OSF510-164 (253.00) This patch corrects the following problems: • Corrects pax/tar/cpio to properly extract explicitly specified files. When an archive contained a file with extended attributes and a different file (occurring later in the archive) was specified to be extracted, improper buffer pointer management resulted in the following display (example uses tar): tar: /dev/nrmt0h : This doesn't look like a tar archive tar: /dev/nrmt0h : Skipping to next file... tar: Memory allocation failed for extended data while reading : Not enough space The directory option was similarly affected. In this case the information for the specified file was not reported • Fixes a problem where the tar -F (Fasttar) option ignores files named err, but does not ignore files named errs or directories named SCCS and RCS.

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

Patch 262.00 OSF510-074B	**Patch:** Fix for loader and ldd **State:** New This patch fixes the following problems: • Fixes a loader problem with rpaths on shared libraries, a loader problem when libraries loaded in -taso mode were loaded above the -taso address range, a problem detecting incorrectly specified _RLD_ARGS values, and a problem handling the RHF_BIND_NOW object file bit. • Fixes a problem with /usr/ucb/ldd. Previously the _RLD_ARGS environment variable was not recognized.
Patch 265.00 OSF510-205B	**Patch:** loader does not report error **State:** Supersedes patches OSF510-028 (78.00), OSF510-147 (263.00) This patch fixes the following problems: • Fixes a problem where applying spike to some binaries results in a 100% performance degradation. • Fixes a problem where spike may fail to delete the low instruction of a pair of related instructions, causing it to abort with a runtime error. • Fixes a problem that may cause the /usr/ucb/spike post-link optimization tool to crash. • Fixes a /sbin/loader problem that causes the ldr_inq_region() call to not report an error when an invalid region parameter is passed as a parameter to the call.
Patch 270.00 OSF510DX-017	**Patch:** Updates Netscape Communicator to Version 4.76 **State:** Supersedes patch OSF510DX-001 (44.00) This patch corrects the following problems: • Fixes a security vulnerability (called the Brown Orifice) in Netscape Communicator Version 4.72 by updating Netscape Communicator to Version 4.75. • Updates Netscape Communicator to Version 4.76 to fix missing default MIME types in Netscape Communicator 4.75.
Patch 280.00 OSF510X11-011	**Patch:** Fixes a memory leak in the X server **State:** Supersedes patch OSF510X11-002 (70.00) This patch fixes the following problems: • Fixes a problem on systems with a PowerStorm 4D10T (ELSA Gloria Synergy, SN-PBXGK-BB) graphics card or a PCI To Ethernet/Graphics Combo Adapter (3X-DEPVD-AA). Sometimes lines and images are not drawn correctly in scrolled windows. • Fixes synchronization and drawing problems in the X server for the PowerStorm 4D10T (ELSA Gloria Synergy, SN-PBXGK-BB) graphics card. • Fixes a memory leak in the X server on systems with a PowerStorm 4D10T (ELSA Gloria Synergy, SN-PBXGK-BB) graphics card that could occur when a client repeatedly created and destroyed buffers for the X Window System Multibuffering Extension (XmbufCreateBuffers/XmbufDestroyBuffers).

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

Patch 283.00 OSF510-104	**Patch:** Security (SSRT0682U) **State:** New. Supersedes patch OSF510-096 (281.00) This patch corrects the following: • Fixes a problem in which rexecd fails to establish stderr. If the client rexec() function call specifies a secondary socket for stderr, connects to rexecd hang. • 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 285.00 OSF510-118	**Patch:** Fixes C++ runtime errors **State:** New This patch fixes C++ runtime errors.
Patch 294.00 OSF510-160A	**Patch:** Fixes a problem with the EVM daemon evmd **State:** New This patch fixes a problem with the EVM daemon, evmd, where it will crash if /etc/rc.config contains a blank line.
Patch 296.00 OSF510-160B	**Patch:** evmd crashes if rc.config contains a blank line **State:** New This patch fixes a problem with the EVM daemon, evmd, where it will crash if /etc/rc.config contains a blank line.
Patch 302.00 OSF510DX-007	**Patch:** dop tool causes segmentation fault **State:** New This patch fixes a problem in which the dop tool would cause a segmentation fault when a non-root user entered the root password.
Patch 304.00 OSF510-137	**Patch:** Running cord on libraries causes infinite loop **State:** New This patch fixes an infinite loop that occurs when using cord on a library compiled with -g3. If the library has unused static routines that are optimized away, cord may go into an infinite loop.
Patch 306.00 OSF510-116	**Patch:** Fixes a C++ compiler error **State:** New This patch fixes a C++ compiler error.
Patch 312.00 OSF510-076	**Patch:** Fixes a problem of the ATM setup script failing **State:** New This patch fixes a problem of the ATM setup script failing when configuring an elan if the lane subsystem is not loaded.
Patch 314.00 OSF510-138	**Patch:** Security (SSRT0708U) **State:** New This patch fixes the following /usr/sbin/inetd problems: • A potential security vulnerability has been discovered, where, under certain circumstances, system integrity may be compromised. This may be in the form of inetd child process core dumping or failing to service incoming connection requests. Compaq has corrected this potential vulnerability. • inetd can terminate without notice and without a core file. • The disable keyword is being ignored when used in the /etc/inetd.conf.local configuration file. • The -h option does not restart any inetd children to handle requests because the parent still thinks one is running.

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

Patch 318.00 OSF510-081	**Patch:** Fix for newgrp command **State:** New This patch corrects the problem where newgrp(1) fails if the file /etc/group contains multiple lines for one group.
Patch 320.00 OSF510DX-011	**Patch:** Fixes a problem in diskconfig **State:** New This fixes a problem in diskconfig where partitions with an offset and size of zero cannot be selected. It also fixes a problem where overlapping partitions cannot be adjusted if the existing partitions are not in alphabetical order.
Patch 324.00 OSF510-142B	**Patch:** Fix for libots3 **State:** New This patch fixes the following problem in the Compaq C compiler: • An optimizer problem that caused a failure in the llogin UNIX command. • An optimizer problem that caused incorrect run-time results for an OpenMP program. • A problem in the parallel processing support library that caused incorrect run-time results for an OpenMP program.
Patch 326.00 OSF510-082	**Patch:** Security (SSRT0672U) **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 330.00 OSF510-135	**Patch:** Write errors occur on soft mounted NFS file systems **State:** Supersedes patch OSF510-070 (132.00) This patch fixes the following problems: • Fixes an NFS file locking race. • Corrects the problem with write errors seen on soft mounted NFS file systems. The error received is: NFS3 RFS3_WRITE failed for server ncinfs: RPC: Server can't decode arguments
Patch 335.00 OSF510-141	**Patch:** Fix for DVD file system problem **State:** New This patch addresses two issues with the DVD File system: • When directory entries are large enough to overflow a user's buffer and require multiple calls to complete, DVDFS fails because it does not properly calculate the continuation point for successive calls. • Logical block numbers are not properly calculated after the first directory data read.
Patch 337.00 OSF510DX-008	**Patch:** Fix for bindconfig **State:** New This patch fixes the problem of OutOfOrder hide stack trace, which occurs when an invalid domain name is entered during bindconfig.
Patch 339.00 OSF510CDE-005	**Patch:** Fix for dtpad **State:** New This patch fixes a problem where, if dtpad cannot allocate enough memory, it will exit and leave a zero-length file in place of the file being edited.

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

Patch 341.00 OSF510-197	**Patch:** Fix for ksh hang **State:** New This patch fixes a problem where the Korn shell (ksh) could hang if the user pastes a large number of commands to it when it is running in a terminal emulator window (such as an xterm).
Patch 343.00 OSF510-114	**Patch:** Fix for vi core dump **State:** New This patch fixes a problem in which the vi editor core dumps when it finds invalid syntax during a substitute operation.
Patch 345.00 OSF510-187	**Patch:** Cannot create builds with CAMDEBUG enabled **State:** New This patch fixes a problem of not being able to create builds with CAMDEBUG enabled.
Patch 347.00 OSF510-079	**Patch:** Fixes a problem of ATM signalling **State:** New This patch fixes a problem of ATM signalling going into connection released after a system reboot.
Patch 349.00 OSF510-121	**Patch:** Corrects memory leak in XTI socket code **State:** New This patch corrects a memory leak in the XTI socket code.
Patch 351.00 OSF510-093	**Patch:** Fix for Turbolaser panic **State:** New This patch prevents a panic on TurboLaser systems with a DE600 in pci slot 0. Mis-identification of the DE600 in pci slot 0 causes data structure corruption. TurboLaser systems include the following: AlphaServer 8200 AlphaServer 8400 AlphaServer GS60 AlphaServer GS60E AlphaServer GS140 A DE600 is a single-port 10/100 Mbps Fast Ethernet NIC.
Patch 353.00 OSF510-190	**Patch:** Fix for fsx utility **State:** New This patch fixes a problem in which the fsx utility would not correctly handle the -s switch.
Patch 360.00 OSF510DX-012A	**Patch:** Nodes in cluster unable to set high temp threshold **State:** New This fix corrects a problem in which nodes in a cluster are unable to set their high temperature thresholds.
Patch 362.00 OSF510DX-012B	**Patch:** Cluster nodes unable to set high temp threshold **State:** New This fix corrects a problem in which nodes in a cluster are unable to set their high temperature thresholds.
Patch 364.00 OSF510-186	**Patch:** Security (SSRT1-15, SSRT0713U) **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 368.00 OSF510-086	**Patch:** rdist utility causes segmentation fault **State:** New This patch corrects a problem in the rdist utility which was causing segmentation faults on files with more than one link.
Patch 372.00 OSF510-127	**Patch:** Kernel memory fault occurs when using tablet **State:** New This patch fixes a kernel memory fault which occurs while using a tablet instead of a mouse.
Patch 374.00 OSF510-139	**Patch:** Hang seen on multi-CPU systems using NFS-over-TCP **State:** New This patch corrects a hang that can be seen on multi-CPU systems using NFS-over-TCP. The SMP race is seen between the nfs_tcp_input and the nfs_tcp_thread functions.
Patch 381.00 OSF510-131	**Patch:** Security (SSRT0664U) **State:** New. Supersedes patch OSF510-100 (379.00) This patch corrects the following: • This patch corrects a problem with the ftpd daemon which could result in PC ftp clients hanging when transferring some files in ASCII mode. • 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 385.00 OSF510-075	**Patch:** Fixes problem in exit status value of swapon utility **State:** Existing This patch fixes a bug in the exit status value of the swapon utility.
Patch 387.00 OSF510-143	**Patch:** CDFS media burned in 2001 shows the wrong dates **State:** New CDFS media burned in 2001 shows the wrong dates.
Patch 391.00 OSF510-128	**Patch:** System crash when accessing the FDI floppy **State:** Supersedes patch OSF510-058 (84.00) This patch corrects the following: • 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 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. • Corrects a potential system crash when accessing the FDI floppy.

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

Patch 393.00 OSF510CDE-007	**Patch:** Fix for CDE window manager loop or abort problems **State:** Supersedes patch OSF510CDE-004 (160.00) This patch corrects the following: • Fixes a problem where the Window Manager (dtwm) intermittently hangs on a system which uses multiple displays. • Fixes a problem where the Common Desktop Environment (CDE) window manager loops or aborts when creating and deleting workspaces or when displaying the CDE Window List.
Patch 397.00 OSF510-222	**Patch:** Fix for grep command **State:** Supersedes patch OSF510-031 (42.00) This patch fixes a problem with the grep command in which the options -p -v together do not produce any output.

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

Patch 408.00 OSF510-242	**Patch:** Fix for vdump problems **State:** Supersedes patches OSF510-013 (13.00), OSF510-161 (175.00), OSF510-285 (406.00) This patch fixes the following problems: • A previous patch caused incomplete restores. • A warning message is displayed when the path for the first file in a group of hard links 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 problems in the vdump command: – Failed to flag compressed extended attributes records that are split across a vdump BLOCK boundary. – Overrides the -D option when source path describes a root fileset (Note: If you want to back up quota files, you must not use the -D option.) – Corrects “Rewinding” message to avoid a segfault with Internationalized messages. – Prevents a core dump from vdump when your message length is greater than MAX_MSG_SIZE. This will be a very rare occurence. – Modifies vdump to forward space to next file only if a norewind tape was specified. • Fixes problems in the vrestore command – Fails to properly handle extended attributes records in compressed archives. This results in malloc failures, proplist corruption, program abort, program crashes due to segfault or invalid memory access, and the display of the error message "error setting extended attributes". – Fails to set extended attributes due to confusion over selective restore of the associated file or directory. Also results in display of the error message "error setting extended attributes". – Selective restore of hardlinked files is incomplete when they exist in different directories (fails to create directory for second occurrence of file with same inode number). – The -Q option is added to vrestore to allow the user to request that quota files are ignored (thus avoiding the time it takes to process them).
Patch 494.00 OSF510-230B	**Patch:** OSF510-230B **State:** New This AdvFS correction makes the balance and rmvol programs more interruptible by supplying a new option (-i). It also avoids wasting extent map entries and avoids a kmf in overlay_xtnt_map.

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

Patch 496.00 OSF510-301	**Patch:** Fix for problems in Compaq C compiler **State:** New. Supersedes patches OSF510-016 (66.00), OSF510-142A (322.00) This patch fixes the following problems: • An optimizer problem that caused the wrong answer to be produced for a program involving tail recursion. • An optimizer problem that caused a runtime error when compiling gcc using -feedback. • An optimizer crash when compiling a program using -ieee and -tune ev6. • An optimizer problem that caused a failure in the llogin UNIX command. • An optimizer problem that caused incorrect run-time results for an OpenMP program. • A problem in the parallel processing support library that caused incorrect run-time results for an OpenMP program. • A compiler problem that caused a runtime failure in specific code that involved floating point arguments and varargs. • A problem in the driver that failed to produce an object file for a command such as: file.s -o file.o • A problem in the driver that would not allow a command line that contained only -l<arg> library and no source or object files. • A problem in the driver that failed to produce an object file when no output file was specified on the command line. • Fixes the following problem in the parallel processing support library (libots3): – A problem in the parallel processing support library that caused incorrect run-time results for an OpenMP program.
Patch 498.00 OSF510CDE-008A	**Patch:** Security (SSRT1-80U) **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 500.00 OSF510CDE-008B	**Patch:** Security (SSRT1-80U) **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 504.00 OSF510-208	**Patch:** Security (SSRT0689U, SSRT1-26) **State:** Supersedes patches OSF510-033 (1.00), OSF510-019 (2.00), OSF510-027 (3.00), OSF510-037A (5.00), OSF510-051 (87.00), OSF510-071 (88.00), OSF510-061 (90.00), OSF510-154 (233.00), OSF510-177 (234.00), OSF510-145 (235.00), OSF510-151 (236.00), OSF510-123 (237.00), OSF510-183 (238.00), OSF510-130 (239.00), OSF510-091 (240.00), OSF510-146 (241.00), OSF510-150 (243.00), OSF510-283 (501.00), OSF510-253 (502.00) This patch corrects the following problems: • Fixes a problem of the getaddrinfo() library call returning a failing status. • Increases the number of places of precision for formatted printing of long doubles. • Fixes the problem that, on rare occasions, the C runtime library atof() and strtod() functions (and other functions that may use them) may produce an incorrect result. The error would only be in the least significant digit of the mantissa (a rounding error). • Fixes hangs in threaded programs with subprocesses created with nfork(NULL). Examining one of the hanging subprocesses shows that it has called fopen() and is waiting for the iobptr mutex in _findiop(). • Fixes the printing of 0.0 when precision is specified for a %g type conversion. • Fixes a problem where a TZ environment variable setting of ":" yields incorrect (or missing) time zone information after calling tzset() and incorrect error reporting from mktime(). • 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 504.00 continued	• Fixes a performance problem with freeing memory in threaded applications, when many allocations of the same size have been made. It also fixes a problem when the __sbrk_override malloc tuning variable is set which caused malloc to try to allocate too much memory. • Fixes a problem with the mallinfo() call which can cause an application to fail if run on a RAD other than 0. • fixes a problem with the mallinfo() call which can cause an application to fail if run on a RAD other than '0'. • Festores correct behavior that existed on pre-V5.0 releases for ecvt() and fcvt(). Floating point exceptions and core dumps no longer occur when denormalized values are passed to ecvt() and fcvt(). • Resolves issues with customer applications that experienced floating point exceptions and core dumps when passing denormalized values to ecvt() and fcvt() that subsequently caused INFORMIX databases to crash. • Fixes the return values for vwprintf() functionality when used with wide characters. • Increases the input buffer size limits for the scanf family of functions to the MAXINT input buffer size. • Fixes the problem of optimized programs printing incorrect values for long doubles. • Adds logic that implements maximum size checks for input width descriptors on numeric scanf() format elements. • Corrects a regular expression performance problem in libc. • Fixes a potential online help build problem when dthelptag is used to compile online help files in a multibyte locale. • Fixes regular expression handling with non-default locale settings. • Fixes a regular expression matching problem in multibyte locales. • Corrects a problem in which the rsh [host] -l [user] [command] command returns "permission denied".

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

Patch 509.00 OSF510X11-022	**Patch:** Fixes an Xserver crash when using GTK **State:** Supersedes patches OSF510X11-010 (246.00), OSF510X11-013 (247.00), OSF510X11-014 (249.00), OSF510X11-003 (119.00), OSF510X11-012 (287.00), OSF510X11-018 (505.00), OSF510X11-020 (506.00), OSF510X11-023 (507.00) This patch fixes the following problems: • Fixes a memory leak in the X server that could occur when a client repeatedly created and destroyed buffers for the X Window System Multibuffering Extension (XmbufCreateBuffers/XmbufDestroyBuffers). • Fixes a problem where the X server does not display windows properly for the 128th and subsequent clients. • Changes the X server to dynamically retrieve its vendor string information when running on COSIX64. • Provides the Xserver library for a new graphics card. • Corrects blocks of erroneous pixels left behind when dragging CDE "pplication manager icons on the desktop. • Fixes a problem that will cause the X server to hang on rare occasions. Except for the mouse, everything on the desktop appears frozen. Output from the ps command will show the X server using greater than 99% of the CPU time. • Fixes an Xserver crash when using the GTK on systems using the Oxygen VX1 graphics card. • Fixes the Xserver problem where, when PanoramiX is enabled and using CDE, icons from dtfile can not be seen on other than the left screen while being moved. • Fixes a problem that can cause CDE pop-up menus to appear on the wrong screen when you are running a multi-head system with the PanoramiX extension enabled.
Patch 513.00 OSF510-317B	**Patch:** Security (SSRT1-40U, SSRT1-41U, SSRT1-42U, SSRT1-45U) **State:** New A potential security vulnerability has been discovere where, under certain circumstances, users can clobber temporary files created by shell commands and utilities (for example, under /sbin, /usr/sbin, /usr/bin, and /etc). Compaq has corrected this potential vulnerability.
Patch 515.00 OSF510-317C	**Patch:** Security (SSRT1-48U) **State:** New A potential security vulnerability has been discovere where, under certain circumstances, users can clobber temporary files created by shell commands and utilities (for example, under /sbin, /usr/sbin, /usr/bin, and /etc). Compaq has corrected this potential vulnerability.
Patch 517.00 OSF510-317D	**Patch:** Security (SSRT1-48U) **State:** New A potential security vulnerability has been discovere where, under certain circumstances, users can clobber temporary files created by shell commands and utilities (for example, under /sbin, /usr/sbin, /usr/bin, and /etc). Compaq has corrected this potential vulnerability.
Patch 519.00 OSF510-244	**Patch:** Installation process does not support alternate root **State:** New This patch fixes a problem with the installation process not supporting alternate root. When a subset is specified on the command line in non-interactive mode, its required subset is incorrectly referenced relative to the default root, not the alternate root.

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

Patch 521.00 OSF510-221	**Patch:** Fix for V5.1 dynamic loader **State:** Supersedes patches OSF510-005 (64.00), OSF510-113 (256.00), OSF510-105 (257.00), OSF510-205A (258.00), OSF510-074A (260.00) This patch fixes the following problems with the V5.1 dynamic loader: • Allows the loader to properly ignore unreferenced symbols when loading a shared library with a dlopen call. • Allows the loader to properly ignore loading a library with the correct library name but an incorrect library version. • Fixes an /sbin/loader problem dealing with absolute value symbols when their value was -1. • Fixes a problem in the /sbin/loader dynamic loader that can cause a crash. It also fixes a problem with the output for the ldd command, where the output was always going to stderr rather than stdout. • A problem that may cause the /usr/ucb/spike post-link optimization tool to crash. • A /sbin/loader problem that causes the ldr_inq_region() call to not report an error when an invalid region parameter is passed as a parameter to the call. • Fixes a loader problem with rpaths on shared libraries, a loader problem when libraries loaded in -taso mode were loaded above the -taso address range, a problem detecting incorrectly specified _RLD_ARGS values, and a problem handling the RHF_BIND_NOW object file bit. • Fixes a problem with /usr/ucb/ldd. Previously the _RLD_ARGS environment variable was not recognized. • Fixes a problem in /sbin/loader. It corrects certain loader failures reported for mismatched shared library versions.
Patch 523.00 OSF510-319	**Patch:** Fix for evmget command **State:** New This patch fixes a situation in which the evmget command and the event log nightly cleanup operation may fail with an "arg list too long" message.
Patch 525.00 OSF510DX-020	**Patch:** Fix for dxarchiver core dump problem **State:** New This patch corrects a dxarchiver core dump problem. The core dump occurs when Clear button is clicked after archiving operation is complete.
Patch 528.00 OSF510-267	**Patch:** Patch: Security (SSRT0690U, SSRT1-40U, SSRT1-48U) **State:** Supersedes patches OSF510-106 (308.00), OSF510-044 (55.00), OSF510-115 (266.00), OSF510-165 (268.00), OSF510-239 (526.00) This patch corrects the following: • Fixes C shell processing problems in the new zh_CN.GB18030 locale. • 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 possible handling problem with multibyte character boundary conditions in ksh script processing. • Fixes two ksh problems that occur in multi-byte Asian locales. • Fixes a problem in which /usr/bin/ksh hangs for certain scripts that contain wait(1).

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

Patch 530.00 OSF510-300A	**Patch:** Fixes POSIX message queue issues **State:** Supersedes patch OSF510-176A (401.00) This patch corrects the following: • Fixes POSIX message queue issues seen with mq_open() and other calls with messsaging. • Fixes a problem that mq_close of a message queue does not call the function p4_delete_entry to free up the resource. Thus, for a process that keeps using mq_open and mq_close, it will eventually run out of descriptors.
Patch 532.00 OSF510-300B	**Patch:** Fix for ERRNO EMFILE 24 error **State:** Supersedes patches OSF510-176C (405.00) This patch corrects the following: • Fixes POSIX message queue issues seen with mq_open() and other calls with messsaging. • Fixes a problem that mq_close of a message queue does not call the function p4_delete_entry to free up the resource. Thus, for a process that keeps using mq_open and mq_close, it will eventually run out of descriptors.
Patch 534.00 OSF510-300C	**Patch:** Fix for POSIX 4 message queue **State:** Supersedes patches OSF510-176B (403.00) This patch corrects the following: • Fixes POSIX message queue issues seen with mq_open() and other calls with messsaging. • Fixes a problem that mq_close of a message queue does not call the function p4_delete_entry to free up the resource. Thus, for a process that keeps using mq_open and mq_close, it will eventually run out of descriptors.
Patch 536.00 OSF510-318	**Patch:** Updates the emx driver to v2.02 **State:** Supersedes patch OSF510-166 (278.00) This patch corrects the following: • Fixes a problem where cascaded switches can hang the system at failover time. • Updates the emx driver to V2.02. – Fixes a problem of unexpected tape I/O aborts. – Fixes a panic of can't grow probe list. – Fixes several kernel memory faults within the driver. – Redundant adapter failures no longer panic the system. – Corrects a problem of panicking with low memory resources. – Corrects stalling I/O during reprobing when a cluster member goes down. – Can't grow list panic which can occur on large fabrics.

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

Patch 538.00 OSF510-274	**Patch:** Fixes problems in the Tru64 UNIX Assembler **State:** Supersedes patches OSF510-132 (288.00), OSF510-103 (290.00) This patch corrects the following: • When assembling a .s file containing a data declaration directive (such as .byte) that specifies a list of values greater than 74, a fatal "yacc stack overflow" condition is raised. • A main procedure's prologue description will overwrite that of an alternate entry point when they both share the same address and they both specify their own .prologue directive. • A .s file that contains .align directives in its text section that is assembled at an optimization level greater than O0 may produce a series of zeros in its text section which, if executed, would cause the program to halt. • The -arch and -tune command line switches were essentially being ignored. • Code generated by the assembler for emulated ldb/ldbu/ldw/ldwu instructions produces incorrect results leading to a linker optimization that produces an invalid executable. • Code generated by the assembler for emulated ldb/ldbu/ldw/ldwu instructions produces incorrect results leading to a linker optimization that produces an invalid executable. • Code generated for loads with offsets larger than 32K is incorrect. • Incorrect addresses are generated when symbolic arithmetic is used, and when the address in question extends beyond the intitial 64K boundary of a section. • A prodecure with no instructions causes the assembler to segfault. • A prodecure with no instructions causes line number generation to segfault. • Data declared using the .gprel32 directive was not being longword aligned. • The relocation count for a program that contains a section that has in excess of 65535 reloctions will be incorrect, resulting in a bad link and an invalid executable. • An entry (PDSC_FLAGS_BASE_REG_IS_FP) was not being set correctly in a short-form stack-frame RPD when a .frame directive specified register 15. • When two entry points to a procedure (main or alternate) share the same address, the assembler generates four nop profiling instruction sequences for each one when the -pg switch is specified. This causes post-link tools, such as spike, problems. • When a main and an alternate entry point share both an address and a prologue, the assembler associates the prologue with the alternate entry and not the main, resulting in the assembler not generating an RPD because it does not see a prologue for the main entry. • The assembler miscalculates the number of relocations present in the .text section if a jmp/jsr instruction was specified without a symbol as an operand. This can result in a linker error.

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

Patch 538.00 continued	• Resolves four incompatibilities between the new (as of V5.1) and old assemblers that are needed to support a future port of gcc to Tru64 UNIX. These changes are included in this version (3.04.33) of the assembler:
	– The assembler has never generated a section header for zero-sized sections, or a symbol table entry for a label symbol that is associated with such a section. This essentially correct behavior represents an incompatibility with the old assembler and has been changed with this patch.
	– The assembler was not including symbols for numeric constant label symbols in the symbol table. It is now.
	– The assembler can produce incorrect scoping for local symbols, resulting in incorrect association of symbols with their containing procedures.
	– The assembler's association of label symbols to their files of origin was incorrect in certain circumstances:
	`.file 1 "file1.cxx"`
	`gcc2_compiled.:`
	`__gnu_compiled_cplusplus:`
	`.file 2 "file2.h"`
	`.file 3 "file3.h"`
	`.text`
	In this example, label1 and label2 are mistakenly associated with file3.h due to the assembler's practice of establishing file context based on the instruction with which a given label was associated, which in this case was the first intruction in the .text section. File context is positional and in this case both labels should be associated with file1.

Patch 540.00 OSF510-250	**Patch:** OSF510-250 **State:** Supersedes patch OSF510-148 (292.00) 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 543.00 OSF510-286	**Patch:** Fixes a panic in the ITPSA driver **State:** Supersedes patches OSF510-004 (128.00), OSF510-210 (298.00), OSF510-217 (541.00) This patch corrects the following problems: • Fixes a cross RAD I/O hang problem with the ITPSA controller. • Fixes a problem that can cause a simple lock timeout or a kernel memory fault on EV6 systems using the ITPSA driver. • Fixes panics associated when multiple KZPCA-AA and/or KZPCM-AA host bus adapters are in the system. The expected panic string is "sc ws remove: SZ_IN_USE NOT set". • Fixes kernel memory faults, and/or I/O hangs with systems that have KZPCM-AA and/or KZPCA-AA. These errors can occur during large data transfers. • Fixes a panic in the ITPSA driver. It is seen when an abort to the SCSI rewind command is issued to a TLZ10 tape device.

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

Patch 546.00 OSF510-330	**Patch:** LAT setup does not handle inittab file as CDSL **State:** New. Supersedes patch OSF510-328 (544.00) This patch corrects the following: • Fixes a problem in latsetup when the directory "/dev/lat" is not found. • Fixes a problem when latsetup does not handle the /etc/inittab file as a Context Dependent Symbolic Link (CDSL).
Patch 548.00 OSF510-245	**Patch:** Fix for lpd hang **State:** Supersedes patch OSF510-080 (300.00) This patch corrects the following: • Introduces the JJ /etc/printcap parameter, which allows the user to choose either one TCP/IP connection for all jobs in the print queue (JJ=1), or a TCP/IP connection for each job in the print queue (JJ=0). It also closes a timing hole that existed when lpd was shutting down. • Fixes a problem in which lpd hangs when printing to advanced server queues (using /dev/null).
Patch 550.00 OSF510-359	**Patch:** JIB graphic card fix **State:** New This patch fixes a problem where, on the ELSA Gloria Synergy, PS4D10, and JIB graphic cards, the cursor position is not being updated properly. The placement of the cursor is one request behind.
Patch 552.00 OSF510-247	**Patch:** Fix for collect command **State:** Supersedes patch OSF510-026 (134.00) This patch corrects the following: • Fixes several problems with the collect command and it adds sysloging when collect suspends, resumes, or receives a signal. • Fixes collect's collector (/usr/sbin/collect) to correctly report the network interface load percentage.
Patch 554.00 OSF510-280A	**Patch:** Fix for class scheduler semaphore race condition **State:** New This patch fixes a class scheduler semaphore race condition.
Patch 556.00 OSF510-280B	**Patch:** Fix for class scheduler problem **State:** New This patch fixes a class scheduler semaphore race condition.
Patch 558.00 OSF510-256	**Patch:** Fixes a volrecover error **State:** New This patch fixes a volrecover error of "Cannot refetch volume" when volumes exist only in a non-rootdg diskgroup.
Patch 561.00 OSF510DX-018	**Patch:** Fixes a core dump problem in dxkerneltuner **State:** New. Supersedes patch OSF510DX-021 (559.00) This patch corrects the following: • Fixes a core dump problem in dxkerneltuner. The core dump occurs when you try to find an attribute (using Find Attributes option under the Options menu) that does not exist. • Fixes a core dump when the dxkerneltuner is used and the Select Subsystem button is pressed twice.

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

Patch 563.00 OSF510-289	**Patch:** Fixes core dump caused by using the rdump utility **State:** Supersedes patch OSF510-003 (68.00) This patch corrects the following: • Fixes a problem where a user could not dump to a regular file. • Fixes a core dump caused by using the rdump utility to back up data.
Patch 565.00 OSF510CDE-009	**Patch:** Fix for palette files not being read **State:** Supersedes patch OSF510CDE-006 (310.00) This patch corrects the following: • Fixes a problem on multi-head systems in which the unlock display only works if the default display is screen 0. • Fixes the problem of palette files not being read from /etc/dt/palettes.
Patch 567.00 OSF510-260	**Patch:** Fixes a kernel memory fault in procfs.mod **State:** Supersedes patch OSF510-171 (316.00) This patch corrects the following: • Corrects a problem where attaching to a program with a debugger will cause periodic timers to be lost and will make the program hang. • Fixes a kernel memory fault in procfs.mod.
Patch 569.00 OSF510-344	**Patch:** Fixes a problem with the disklabel command **State:** New This patch fixes a problem with the disklabel command. Disklabel was displaying large unsigned values as negative numbers.
Patch 571.00 OSF510-219	**Patch:** Fix for mv command **State:** New This patch fixes a problem in which the mv command will not perform a move if the inode of the file is the same as the inode of the destination directory, even though said file and directory are on different file systems.
Patch 573.00 OSF510-336	**Patch:** Fixes a NetRAIN problem **State:** New This patch fixes a problem in netrain. NetRAIN interface creation now fails if any of the requested standby interfaces do not exist.
Patch 575.00 OSF510DX-019	**Patch:** Allows the dxsetacl utility to delete access ACLs **State:** New This patch allows the dxsetacl utility to delete access ACLs.
Patch 577.00 OSF510-234	**Patch:** Fixes the consumption of excessive CPU cycles **State:** New This patch fixes the consumption of excessive CPU cycles caused by rshd when SIA is enabled.
Patch 579.00 OSF510-342	**Patch:** Fixes a problem with the 400ms delay **State:** New This patch fixes a problem with the 400ms delay upon network cable reinsertion which could lead to temporarily held drivers.

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

Patch 581.00 OSF510DX-022	**Patch:** Security (SSRT1-40U, SSRT1-41U, SSRT1-42U, SSRT1-45U) **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 583.00 OSF510-257	**Patch:** Kernel leaves cached pointers to ksm data structure **State:** Supersedes patch OSF510-020 (21.00) This patch corrects the following: • Corrects a stack overflow panic encountered during the startup of the system management deamon(smsd) on configurations with more than 255 devices. • Fixes a problem within the kernel that could leave cached pointers to a ksm data structure after the ksm instance was removed from the hierarchy. A kernel memory fault or data inconsistency could result.
Patch 585.00 OSF510-284	**Patch:** Fixes a problem with the keyboard driver **State:** New This patch fixes a problem where the keyboard driver takes too long probing for the keyboard when a keyboard is not connected.
Patch 587.00 OSF510-308	**Patch:** Security (SSRT0743U, 88914, SSRT0743U) **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 589.00 OSF510-270	**Patch:** Fix for sort command **State:** New This patch corrects the behavior of the sort(1) command which now checks for duplicates with -c, -u, and -k flags.
Patch 591.00 OSF510-215	**Patch:** Fixes several problems found in the KZPEA driver **State:** Supersedes patch OSF510-041 (57.00) This patch corrects the following: • Fixes a panic or a system hang which could occur on a DS20E with drives attached to the motherboard SCSI interface (Adaptec 7895 based) or on an Ultra3 KZPEA SCSI adapter. In addition to system hangs or panics on configurations using Memory Channel adapters some configurations have exhibited SCSI device problems. • Fixes several problems found in the KZPEA driver that could result in memory corruption, bus hangs, and system panics. This patch also includes binary error logging support in the driver.
Patch 593.00 OSF510-349	**Patch:** Fixes a potential race deadlock **State:** New This patch fixes a potential race deadlock between vclean/ufs_reclaim and quotaon/quotaoff, when quota is enabled.
Patch 595.00 OSF510-223	**Patch:** Fixes a bug that causes a panic due to software error **State:** New This patch fixes a bug that would cause a panic due to a software error that removed some functionality in system security.

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

Patch 598.00 OSF510X11-015A	**Patch:** Security (SSRT0638U) **State:** New. Supersedes patch OSF510X11-017A (596.00) 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 root directory compromise via lpr using X11. • Allows the dxsetacl utility to delete access ACLs.
Patch 600.00 OSF510X11-017B	**Patch:** Security (SSRT0638U) **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 root directory compromise via lpr using X11.
Patch 602.00 OSF510X11-015B	**Patch:** Fix for dxsetacl utility **State:** New This patch allows the dxsetacl utility to delete access ACLs.
Patch 605.00 OSF510-240	**Patch:** Fix for ld -f command **State:** Supersedes patches OSF510-022 (72.00), OSF510-153 (354.00), OSF510-108 (355.00), OSF510-120 (356.00), OSF510-102 (358.00), OSF510-258 (603.00) This patch corrects the following: • Fixes a spike problem. The problem results in an assertion and core dump when trying to spike a kernel. This patch is only needed if the post-link tool spike will be used on the Tru64 UNIX kernel. • Fixes a problem where the linker defined symbol _fpdata would end up being undefined if it was referenced by a program but not used by the linker. • Fixes link errors encountered when linking with -A. • Fixes two problems in the linker where it would erroneously report "multiply defined symbol" errors or "unresolved symbol" errors. – Modifies the linker's symbol resolution to enable it to recognize when a reference to a symbol defined in a shared library is replaced by a symbol defined in an object file or archive. – Modifies the linker to cause it to rescan shared libraries before reporting unresolved symbols. • Fixes two errors that occur when using the -f switch with the linker (ld): – Using the -f switch produces link errors. – Any unsupported switch beginning with -f gets interpreted to mean -f. • Fixes a potential optimization problem with the linker (/bin/ld). • Fixes a linker failure that can occur when linking a -non_shared executable with libexc.a.
Patch 607.00 OSF510-233	**Patch:** Fix for line printer problem **State:** New This patch fixes a loss of data with the parallel line printer driver. Without this patch data from a print job may get dropped if multiple jobs are sent to the line printers in rapid succession.

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

Patch 609.00 OSF510-238	**Patch:** Fix for cp command **State:** New This patch fixes a problem in which cp(1) and cat(1) produce different file sizes when reading from a tape device. The solution was to change the I/O buffer size of the cp command from 64K to 8K.
Patch 612.00 OSF510-312	**Patch:** Fix for kernel memory fault when using ATM **State:** Supersedes patches OSF510-056 (126.00), OSF510-338 (610.00) This patch corrects the following: • When running ATM LAN Emulation, using more than 4 ATM NetRAIN interfaces can result in recursive calls causing a "kernel stack not valid" halt. • Corrects a problem which could result in ATM/lane connection requests being dropped. • Fixes a kernel memory fault when using ATM.
Patch 614.00 OSF510-265	**Patch:** Support added for fixfdmn utility **State:** New This patch provides support for the /sbin/advfs/fixfdmn utility. The /sbin/advfs/fixfdmn utility is a tool that is used to check and repair corrupted AdvFS domains.
Patch 616.00 OSF510X11-016A	**Patch:** OSF510X11-016A **State:** Supersedes patches OSF510X11-004A (135.00), OSF510X11-008A (137.00) This patch corrects the following: • Fixes two memory leaks in the X Window System's X library (Xlib) that can occur when creating and destroying Motif List, Text, and TextField widgets. • Provides enhanced support for UTF-8 and UCS-4 locales. • Fixes a problem with libX11.a and libX11.so that might cause a core dump by failing to initialize some variables in some Xlib internal functions.
Patch 618.00 OSF510X11-016B	**Patch:** Fix for libX11.a and libX11.so core dump problem **State:** Supersedes patches OSF510X11-004B (138.00), OSF510X11-008B (140.00) This patch corrects the following: • Fixes two memory leaks in the X Window System's X library (Xlib) that can occur when creating and destroying Motif List, Text, and TextField widgets. • Provides enhanced support for UTF-8 and UCS-4 locales. • Fixes a problem with libX11.a and libX11.so that might cause a core dump by failing to initialize some variables in some Xlib internal functions.
Patch 620.00 OSF510-252	**Patch:** Security (SSRT1-85U) **State:** New A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. xntpd contains a potential buffer overflow that may allow unauthorized access to bin privileges. Compaq has corrected this potential vulnerability.
Patch 622.00 OSF510-220	**Patch:** Fix for rerouting problem seen on a cluster **State:** New This patch fixes a problem where pulling the network cable on one node acting as a CFS server in a cluster causes no rerouting to occur.

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

Patch 624.00 OSF510-254	**Patch:** Log in requests hang when enhanced security enabled **State:** Supersedes patches OSF510-054 (145.00), OSF510-055 (146.00), OSF510-072 (148.00), OSF510-170 (370.00) This patch corrects the following: • Corrects a problem in an Enhanced Security configuration where, at login time, if it is determined an account's password has expired, the "Old password:" prompt did not appear. Rather, the user is immediately prompted for their new password options and is allowed to change to a new password. This patch also allows a user logged into a system configured as a NIS client with Enhanced Security installed to change their password. • Fixes a problem in an Enhanced Security configuration. This patch restores the capability of being able to su to a user as root without being prompted or having to know the users password. • Fixes a problem for Enhanced Security configurations where the Maximum Login Interval (u_max_login_intvl) field was being ignored for account templates. • Fixes problems with the prpasswdd daemon hanging when there are numerous background processes simultaneously attempting to authenticate users to the system in an Enhanced Security environment. • Fixes a problem in which login requests can hang when enhanced security is enabled.
Patch 626.00 OSF510-236	**Patch:** Fix for the i2c kernel module **State:** Supersedes patch OSF510-172 (376.00) This patch corrects the following: • Fixes DS10/DS20 performance problems introduced with the i2c driver by using thread blocking, rather than event_timeout() and DELAY(). • Fixes various inefficiencies in the i2c kernel module, and fixes a lock hierarchy violation that could be seen with the generic kernel attribute lockmode turned on.
Patch 628.00 OSF510-340	**Patch:** BPF default packet filter causes system panic **State:** New This patch corrects a problem which could result in a system panic on close() if the BPF default packet filter is in use.
Patch 630.00 OSF510-309	**Patch:** Fixes streams based drivers from failing **State:** Supersedes patch OSF510-077 (378.00) This patch corrects the following: • Fixes a problem in which the system may panic with the panic string "Unaligned kernel space access from kernel mode". • Fixes streams based drivers from failing DRV_GETHANDLE, due to non supported driver_handle.
Patch 632.00 OSF510X11-019	**Patch:** Fixes problems with X server X Image Extension **State:** New This patch fixes problems with the X server X Image Extension (XIE).

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

Patch 634.00 OSF510-331	**Patch:** Security (SSRT1-40U, SSRT1-41U, SSRT1-42U, SSRT1-45U) **State:** Supersedes patches OSF510-185 (331.00), OSF510-112 (333.00), OSF510-317A (511.00) This patch corrects the following problems: • Fixes errors generated by syscheck when NFS is not configured. • Upgrades sys_check to V120. • A potential security vulnerability has been discovered where, under certain circumstances, users can clobber temporary files created by shell commands and utilities (for example, under /sbin, /usr/sbin, /usr/bin, and /etc). Compaq has corrected this potential vulnerability. • Provides the /usr/lbin/mkstemp program which allows the mechanism to create a secure temporary file.
Patch 636.00 OSF510-273	**Patch:** Corrects problems with joind **State:** Supersedes patch OSF510-152 (389.00) This patch corrects the following: • Corrects a problem with joind which caused it to respond to certain client dhcp requests via the wrong port. • Fixes a problem where joind may fail to clean up its lock files in /var/join.
Patch 638.00 OSF510-327	**Patch:** Security (SSRT0713U) **State:** Supersedes patch OSF510-189 (395.00) 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 problems that may prevent a correct configuration table entry from being written to the binary error log on some systems, and may cause binlogd to display error messages on others.

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

Patch 647.00	**Patch:** Fixes ee driver for DE60x Ethernet cards
OSF510-390	**State:** Supersedes patches OSF510-174 (250.00), OSF510-173 (252.00), OSF510-025 (59.00), OSF510-042 (156.00), OSF510-048 (53.00), OSF510-010 (60.00), OSF510-014 (62.00), OSF510-015 (151.00), OSF510-087 (152.00), OSF510-060 (154.00), OSF510-011 (11.00), OSF510-032 (22.00), OSF510-006 (23.00), OSF510-007 (24.00), OSF510-008 (25.00), OSF510-049 (26.00), OSF510-030 (27.00), OSF510-012 (28.00), OSF510-023 (29.00), OSF510-047 (30.00), OSF510-039A (32.00), OSF510-059 (86.00), OSF510-065 (93.00), OSF510-073 (94.00), OSF510-084 (95.00), OSF510-063 (96.00), OSF510-053 (97.00), OSF510-050 (98.00), OSF510-064 (99.00), OSF510-035 (100.00), OSF510-062 (101.00), OSF510-089 (103.00), OSF510-095 (163.00), OSF510-094 (165.00), OSF510-101 (167.00), OSF510-097 (176.00), OSF510-119 (177.00), OSF510-110 (178.00), OSF510-124 (179.00), OSF510-175 (180.00), OSF510-078 (181.00), OSF510-159 (182.00), OSF510-196 (183.00), OSF510-107A (184.00), OSF510-126 (185.00), OSF510-182 (186.00), OSF510-201 (187.00), OSF510-213 (188.00), OSF510-168 (189.00), OSF510-212A (190.00), OSF510-211 (191.00), OSF510-111 (192.00), OSF510-184 (193.00), OSF510-188 (194.00), OSF510-099 (195.00), OSF510-149 (196.00), OSF510-206A (197.00), OSF510-136 (198.00), OSF510-209 (199.00), OSF510-140 (200.00), OSF510-117 (201.00), OSF510-192 (202.00), OSF510-089 (103.00), OSF510-095 (163.00), OSF510-094 (165.00), OSF510-101 (167.00), OSF510-097 (176.00), OSF510-119 (177.00), OSF510-110 (178.00), OSF510-124 (179.00), OSF510-175 (180.00), OSF510-078 (181.00), OSF510-159 (182.00), OSF510-196 (183.00), OSF510-107A (184.00), OSF510-126 (185.00), OSF510-182 (186.00), OSF510-201 (187.00), OSF510-213 (188.00), OSF510-168 (189.00), OSF510-212A (190.00), OSF510-211 (191.00), OSF510-111 (192.00), OSF510-184 (193.00), OSF510-188 (194.00), OSF510-099 (195.00), OSF510-149 (196.00), OSF510-206A (197.00), OSF510-136 (198.00), OSF510-209 (199.00), OSF510-140 (200.00), OSF510-117 (201.00), OSF510-192 (202.00), OSF510-362 (415.00), OSF510-377 (416.00), OSF510-353 (417.00), OSF510-229 (418.00), OSF510-302 (419.00), OSF510-232 (420.00), OSF510-251 (421.00), OSF510-365 (422.00), OSF510-341 (423.00), OSF510-241 (424.00), OSF510-218 (425.00), OSF510-321 (426.00), OSF510-294 (427.00), OSF510-360 (428.00), OSF510-345 (429.00), OSF510-259 (430.00), OSF510-299 (431.00), OSF510-372 (432.00), OSF510-231 (433.00), OSF510-296 (434.00), OSF510-339 (435.00), OSF510-293 (436.00), OSF510-304 (437.00), OSF510-230A (438.00), OSF510-354 (439.00), OSF510-305 (440.00), OSF510-228 (441.00), OSF510-355 (442.00), OSF510-237 (443.00), OSF510-227 (444.00), OSF510-306 (445.00), OSF510-202 (446.00), OSF510-383 (447.00), OSF510-282 (448.00), OSF510-272 (449.00), OSF510-352 (450.00), OSF510-287 (451.00), OSF510-316 (452.00), OSF510-311 (453.00), OSF510-346 (454.00), OSF510-314 (455.00), OSF510-356 (456.00), OSF510-303 (457.00),

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

Patch 647.00 continued	OSF510-295 (458.00), OSF510-292 (459.00), OSF510-335 (460.00), OSF510-291 (461.00), OSF510-281 (462.00), OSF510-279 (463.00), OSF510-320 (464.00), OSF510-243 (465.00), OSF510-278 (466.00), OSF510-288 (467.00), OSF510-263 (468.00), OSF510-255 (469.00), OSF510-248 (470.00), OSF510-268 (471.00), OSF510-369 (472.00), OSF510-357 (473.00), OSF510-374 (474.00), OSF510-332 (475.00), OSF510-310 (476.00), OSF510-364 (477.00), OSF510-333 (478.00), OSF510-358 (479.00), OSF510-271 (480.00), OSF510-290 (481.00), OSF510-235 (482.00), OSF510-298 (483.00), OSF510-326 (484.00), OSF510-269 (485.00), OSF510-249 (486.00), OSF510-350 (487.00), OSF510-337 (488.00), OSF510-323 (489.00), OSF510-264 (490.00), OSF510-307 (492.00), OSF510-389 (639.00), OSF510-388 (640.00), OSF510-386 (641.00), OSF510-387 (642.00), OSF510-390 (644.00), OSF510-413 (645.00) This patch corrects the following problems: • Corrects a problem where a race condition in NFS can result in a kernel memory fault. • Fixes a problem where threads can hang while renaming files on NFS mounted file systems. • This patch avoids tagged-file induced automount requests in AutoFS. • This patch is required in order to use the SuperDLT1 tape drive. • Fixes a problem encountered on a heavily loaded HSG80, in which a device may become unavailable to other cluster members if a cluster node crashes at the same time an error occurs on that device. • Prevents panics from occurring if AdvFS detects corruption in the per-fileset frags file and attempts to work around the corruption. • Fixes AdvFS memory mapped file support so that it honors the noatimes and readonly mount options when updating file timestamps. • A kernel memory fault can occur on an smp machine when one thread is extending a clone frags file and another thread does a stat system call on a file with a frag. • Provides an improvement to AdvFS performance when the first bytes of user data (and subsequent storage requests) is written to a domain. • Corrects read-ahead behavior for AdvFS for both local and NFS reads. Read performance is increased by approximately 10% with the addition of this patch. This patch does not include any correctness fixes. • Fixes a problem on AlphaServer GS80, GS160, and GS320 systems where, under a specific set of unlikely circumstances, it is possible for Revision 4 PCA hardware to falsely report PCI hung bus errors. This will cause a uncorrectable hardware machine check and operating system panic. This patch must be installed if the hardware configuration includes any Revision 4 PCA (IOP to PCI bus) adapters. • Fixes a kernel memory fault which can occur during scheduler load balancing on a NUMA system.

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

Patch 647.00 continued	• Fixes a panic that occurs in madvise() when called with MADV_DONTNEED when running in lockmode 4. • Improves performance of HPTC programs on GS-series NUMA machines. • Fixes a kernel memory fault which can happen when all the physical memory is in use. • Fixes a problem seen in a cluster when one member whose boot partition is on a device whose SCSI wwid changes while the node is down. • Corrects a failure that is seen as a user_cmd timeout. • Fixes a kernel memory fault when accessing a shared text segment after or during load balancing on a NUMA system. • Fixes a bug that, when fuser -k is issued on a dismounted NFS mount point in which a process is running, a hang will occur. • 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. • Improves webserver performance, fixes an IPV6 related crash, and a hang in soclose(). • Fixes problems for threaded applications running on Tru64 UNIX V5.1 • sbin/dd has been made non-threaded. This is to avoid problems while installing patches that are incompatible with the running kernel. /usr/bin/dd is not affected by this patch. • Fixes SPECweb99 httpd hangs in umc_get_page() routine waiting for the page. • Includes performance fixes for systems doing raw I/O, raw async I/O, and systems with large disk farms (high disk count). • Enables the getconf command to return the abbreviated vendor name correctly. • Provides the device driver for a new graphics card. • Fixes a problem where some network-based multimedia applications will cause a kernel memory fault when exiting. • Provides support for the DEGPA-TA (1000BaseT) Gigabit Ethernet device. • Fixes a potential deadlock on systems using shared memory segments and granularity hints. This can occur when allocating a gh region larger than the available free memory. • Improves UDP performance by removing an unneeded lock from the UDP output path. • Fixes a panic in in_pcbfree() when NFS is implemented over TCP. • Fixes a lock contention for multiple writers which would use 100% of CPU time. This problem has been seen when running Oracle database doing Table Creates. • Resolves hang-like behavior when LSM volumes are used to create AdvFS domain volumes. The default preferred I/O byte transfer size may be too large and needs to be set lower. • Fixes periodic slowdowns seen on large systems that are consuming large amounts of memory due to file I/O. These changes make the reclaiming of memory in use for file buffers more efficient. There is also a fix for a lock timeout seen on the vdIoLock because of a large number of buffers on the SmoothSync queues.

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

Patch 647.00 continued	• Fixes a race condition which could result with either a Kernel Memory Fault or a Kernel Unaligned Access in one of the AdvFS I/O queue manipulation routines. • Fixes inaccuracy problems when using setrlimit/getrlimit with a threaded application. • Addresses multiple issues for the KZPCC family of RAID Array 2000 (RA2000) controllers: – Errors seen when concurrent opens are issued to separate logical partitions on the same logical device. – Change to the preferred chunk size from 16 KB to 64 KB which may increase data transfer rates. • Fixes a hang seen while running collect and the vdump utility. This patch prevents the hang in tok_wait from occurring. • Prevents stat(), lstat(), fstat(), statfs(), fstatfs(), getmntinfo(), and getfsstat() from returning EOVERFLOW errors for programs compiled on Tru64 UNIX V4.0 or earlier. • Fixes a problem where threads can hang in x_load_in-mem_xtnt_map(). • Fixes a kernel memory fault when writing to /proc, while anon_rss_enforce is set to 2. • Fixes an issue with lightweight wiring of pages and shared memory regions. • Fixes a system panic when the system has at least one AdvFS domain and the system is configured for lockmode=4 kernel lock statistics collection. • Corrects some I/O rate fluctuations and thread unresponsiveness that had been seen when vm free pages dropped to a low level and used pages were being recycled. • In laboratory testing Compaq has observed that, under certain circumstances, a possibility exists that inconsistent data may be written to disk on some Tru64 UNIX V5.0A and V5.1 systems running AdvFS and direct I/O. Compaq became aware of this possibility only during laboratory testing. To our knowledge, no customer has experienced this problem. Compaq is alerting customers to this potential problem as a precautionary measure. The conditions under which this potential problem may occur are as follows: – An application writes to a file using AdvFS direct I/O and the file had previously been opened for normal I/O (which by default is cached). – Some but not all of the pages are still resident in Unified Buffer Cache (UBC) memory. Invalid data could occur when a single direct I/O write spans multiple AdvFS pages, and some, but not all, of the pages are still in the UBC. If the file has been opened only for direct I/O and remains open for direct I/O, the problem does not exist. Applications that use direct I/O, such as Oracle, could be affected. • This patch addresses two types of system crashes: – Crash caused by VM hash corruption, kernel memory fault. – Crash caused by a lock hierarchy violation.

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

Patch 647.00 continued	• Fixes a problem with the driver for Gigabit Ethernet adapters (DEGPA-FA and DEGPA-TA) which prevented its use in a NetRAIN (Redundant Array of Independent Network Adapters) set. • Fixes a problem where the setgid bit of a directory was not being set when created if its parent directory has the setgid bit set. • Fixes issues with memory allocation attributes. • Fixes a bug in the POSIX Threads Library for Tru64 UNIX V5.1 where a terminating thread did not properly clear an enabled floating point unit, causing an invalid floating point state on the next thread that was run. • Fixes several virtual memory algorithms related to the allocation and freeing of pages within the kernel. • Fixes panics which can occur if a signal is sent to a multi-threaded task in which one or more threads are calling exit() or exec(). • Fixes the corruption of the CAM hardware database when using hwmgr. This typically can result in a kernel memory fault when the database is being written to disk after a hwmgr operation. • Corrects an AdvFS panic which can occur during a rmfset operation, causing the following panic string: rbf_delete_int: can't find bf attributes • Fixes an issue with some remote ioctls for tape/changer drivers not working in a cluster. • Fixes a panic which comes from a page fault on a user buffer while already holding the write lock. • Fixes a bug in the POSIX Threads Library for Tru64 UNIX V5.1 that would result in a DECthreads error return of EINVAL from the pthread mutex API routines. This error would be seen only when the thread stack had been user defined/changed, specifically seen when using the user level context switching (ucontext) routines. • Fixes a problem in which the system panicked with a kernel memory fault while the class scheduler was being configured. • Fixes cluster hangs where I/O stops, and a hwmgr -view -clu command does not return. However, the systems will respond to pings. This is caused by the ubc_memory_purge in routine cfs_putpage being blocked when doing FSOP_PUTPAGE.

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

Patch 647.00 continued	• Fixes the following system panics: – A "simple_lock: lock already owned by cpu" panic when anon_rss_enforce is non-zero and lockmode is set to 4. This remove occurs when a process, whose RSS (resident set size; the number of pages a process can have in memory) limit is exceeded tries to expand its heap. – A "panic: vm_page_activate: already active" panic that can occur on a system during memory shortages. – An "mcs_lock: no queue entries available" panic that can occur on a GS160 system. This is caused by an abandoned page mistakenly being reclaimed off the the 0/O hash. The page is then removed off a UBC free list where two stale page pointers were connected, hereby connecting the ACTIVE and INACTIVE list. When attempting to deactivate pages (move them from the ACTIVE queue to the INACTIVE queue) an INACTIVE page is encountered, which causes an inadvertant failure to unlock the page. Continued attempts to deactivate INACTIVE pages results in the lock queue being filled. This can also cause a "kernel memory fault" panic. • Fixes a problem in which a heavy load placed on an HSG80 can disable the device. • Fixes a timing window where flushing data to disk can be incomplete when a system is going down, or if more than one thread calls reboot() without first going through shutdown, /sbin/reboot, or /sbin/halt. • Fixes a system crash that could occur when calling nmadvise. • 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. • Eliminates a kernel memory fault in AdvFS. • Fixes multiple problems with SCSI tape handling including improvements to backup procedures, SCSI passthrough, an increase to the local IO size for transfers, a fix for a system crash that can occur during a bus reset, and a fix for a panic with the following panic string: PWS_CCB_QUE_REMOVE: CCB NOT ON ANY LIST • Fixes a system hang caused by netisr queue corruption due to a race condition that is primarily encountered by third party drivers and layered products that call schednetisr_nospl(). • Fixes a lockmode 4 panic in netisr_del_rad where netisr_del_rad attempted to release a lock it did not hold. • Corrects the use of Granularity Hints in a threaded application program. • Fixes a problem with writing out crashdumps on systems with their swap on FibreChannel.

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

Patch 647.00 continued	• Fixes a kernel memory fault and invalid memory ifetch panic which can occur in AlphaServer SC systems running Quadrics' RMS software. • Addresses two problems with the ee driver for DE60x Ethernet cards. These problems affect all Tru64 UNIX systems containing ee cards: – Fixes a race condition where the card could stop receiving packets from the network under rare circumstances. – Fixes the lan_config user options -x and -s. • Fixes some problems seen with loading and unloading dynamic drivers. • Fixes a couple of problems in NFS that can cause a kernel memory fault during NFS server shutdown. • Corrects a problem with ICMP redirect processing which resulted in incorrect ICMP redirect messages. • Fixes a kernel memory fault when performing asynchronous input/output over sockets. • Fixes several bugs related to shared memory (memory that can be accessed by more than one cpu) that could lead to panics, hangs and performnace problems. • Fixes a problem with sendmsg and rcvmsg that prevented 9i/RAC from being able to use UDP as its transport. With this patch, correct operation of sendmsg and rcvmsg is restored when dealing with atomic protocols by not truncating send but to treat as a 32 bit length. • Fixes a kernel memory fault in mount -o extend. • Provides a script, /usr/sbin/clone_versw_undo, that will allow a user to remove the directio cloning patch after the version switch has been thrown by running clu_upgrade -switch. This script will set back the version identifiers and request a cluster shutdown and reboot to finish the deletion of the patch. Another rolling upgrade will be required to delete the patch with dupatch. • Fixes a rare panic in the driver for the DE600/DE602 10/100 Ethernet adapter. • Fixes data inconsistency problems that can be seen on clusters that are NFS clients.

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

Patch 647.00 continued	• Fixes a misconfiguration of vm_free_target at the boot time when this parameter is added to /etc/sysconfigtab. • Fixes problems seen with the loading and unloading of dynamic drivers. • Fixes a kernel memory fault in tcp_rad_slowtimo. This patch also fixes a kernel memory fault in soclose() before calling soabort for listener sockets. • Fixes a crash when an AdvFS filesystem reports I/O errors and enters into a domain panic state. AdvFS's error cleanup would panic on an invalid pointer and report an "invalid memory read access from kernel mode" panic message. • Fixes a time loss problem seen on DS systems (TSUNAMI) only when using console callbacks. The patch resynchronizes the clock when a time loss is detected. • Prevents the error message "local HSM Error: msgsvc: socket close failed" from being generated when an application closes the socket with return state 0. • Fixes a problem in which activity to a disk that is connected to an HSG80 will hang if the disk is removed and reinserted. • Prevents a potential hang due to external NFS servers. • Fixes a panic in ubc_page_release while running direct I/O. The fix ensures that even pre-allocated pages get flushed, thus preventing an lru corruption. • Fixes a problem where, when using VX1 graphics module, the mouse cursor disappears when moved along the left and topmost edges. • Fixes a system panic with "malloc_check_checksum: memory pool corrution" message. • Corrects several problems in kernel routing: – Fixes a panic when deleting an IP address. – Fixes a panic when performing IP re-configuration. – Adds interface route on address configuration. • Corrects a problem in the virtual file system that could cause panic with the panic string "kernel memory fault."

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

Patch 647.00 continued	• Fixes a bug between mcs_unlock and mcs_lock_try on the same CPU, causing the mcs_unlock to hang. • Ensures that if an AdvFS file is opened for both O_DIRECTIO and O_APPEND, threads racing to append data to the file will be correctly synchronized, and all data will be appended to the file. • Fixes a bug in virtual memory that can cause a kernel memory fault. • Fixes a condition where the smoothsync thread, in attempting to flush dirty buffers for memory-mapped files, would also flush buffers for non-memory-mapped files. This did not cause any errors, but could cause more I/O than necessary. • Fixes a potential problem with lost data after a direct I/O write with a file extension followed quickly by a system crash. • Fixes a kernel panic with the following message: bs_invalidate_rsvd_access_struct: bad access struct • Makes the balance and rmvol programs in AdvFS more interruptible by supplying a new option (-i). It also avoids wasting extent map entries and avoids a kmf in overlay_xtnt_map. • Fixes the following problems: – The system may hang while attempting to replace a component that is used in a redundant configuration. – The system may experience a kernel memory fault when an I/O path is removed. Just before the panic occurs, you may see: Jun 24 16:21:05 tstsys vmunix: DDR - Warning: Device has no "name" - for Jun 24 16:21:05 tstsys vmunix: Vendor ID : Product ID: • Fixed kernel memory fault when use open a command hwmgr -delete component -id 3. • Fixes a problem that would cause a process to hang because the process was unable to exit. • Eliminates superfluous AutoFS auto-mount attempts during rolling upgrade. These attempted auto-mounts slow down certain operations and leave the AutoFS namespace polluted with directories prefixed with .Old.. • Fixes some problems with the mkdir -p command when executed on automount directories. • Fixes a problem where a long-running kernel thread in AdvFS could cause a cluster timeout and subsequent panic. It also fixes a simple_lock timeout panic.

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

Patch 647.00 continued	• Corrects a problem with the network code which resulted in some tcp packets having the wrong checksums. This could result in dropped connections. • Fixes lock time issues, UBC performance problems, and provides AdvFS and UFS performance improvemnts in platforms, other than Wildfire, with low memory. • Fixes a problem with AdvFS that, when mounting the filesystem with option -o dual a panic is caused. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This could result in a panic with the string: "lock_clear_recursive: recursion not enabled". Compaq has corrected this potential vulnerability. • Fixes a panic seen on a cluster that displays the panic string "mcs_lock: time limit exceeded". In the dump you will see both dyn_lock_bucket and dyn_hash_obtain_chain. • Fixes a kernel memory fault caused by AutoFS. • The table() system will not abort connections properly if a tcb hash table number is greater than 1. • Corrects an "mcs_lock: time limit exceeded" panic when moving processors to/from processor_sets. • Fixes a bug that can cause performance problems for certain applications when the sysconfigtab parameter ipc:sem_broadcast_wakeup is set to 0. • Fixes several directIO problems seen when using the aio interface. The symptoms include a kernel memory fault, and an aio condition that causes a live_dump to be generated. • Fixes the following Virtual Memory problems. The first three are seen on NUMA systems only, and the fourth problem can be seen on any system type: – A "vm_pg_alloc: page not free" system panic that occurs during process migration. – A "vm_pageout_activate: page already active" system panic that occurs if one thread is unlocking some pages in memory while another thread is migrating them. – Memory inconsistancies caused by fault path for large shared memory regions prematurely releasing a hold on a page it just locked. This can cause variety of problems including user program errors and system panics. – A "simple_lock: time limit exceeded" system panic that occurs if very large (8MB or larger) System V Shared memory regions are in use.

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

Patch 647.00 continued	• Corrects the problem of a simple lock timeout due to POSIX timers and also corrects some inaccuracies of the POSIX realtime timers. • Fxes a kernel memory fault in msg_rpc_trap. • Fixes a problem where the I/O transfer rate can suddenly drop when writing to a hole in a large file in an AdvFS domain, when a volume in that domain becomes full. • Fixes a panic with the following error message: panic: cfsdb_assert • Prevents a hang in msfs_cfs_flush_and_invalidate() when running defragment on a cluster. • Fixes a problem such that applications that directly manipulate memory buffer pointers get correct results. This problem is exhibited when using Tarantella Enterprise 3 application server software to run applications. The UNIX system will hang, requiring a power shutdown and system reboot to recover. • This patch will fix panics generated by whole-file flushes of metadata files. Symptoms include: CLUSTER BOOT PANIC: SIMPLE_LOCK: UNINITIALIZED LOCK KMF IN ADVFS_PAGE_BUSY() DURING RECOVERY PROCESSING PANIC WHEN MOUNTING ADVFS FILE SYSTEM ADVFS CLUSTER ROOT DOMAIN GOT CORRUPTED • Replaces the system panics caused by "Can't clear bit twice" with a domain panic. • The mkfdmn command now works with the -V3 and -p options. This prevents a core dump from being generated. This is a rare situation that was seen by code inspection. • Domain panics that were inadvertently removed from bs_frag_alloc() have been replaced. • A potential security vulnerability has been discovered in the kernel where, under certain circumstances, a race condition can occur that could allow a non-root user to modify any file and possibly gain root access. • Fixes a problem in which netisr_add() can erroneously return an EEXIST error. This problem can manifest as "Framework error: connection problems" messages from X.25 applications.

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

Patch 647.00 continued	• Addresses a panic situation in IN_PCBREF and a change to tcp_deletetcb to prevent a crash. • Corrects several CAM errors including: passthru IOCTL fails with EIO (CAM_BUSY) problem; RESERVATION CONFLICT driver BUSY problem; enforce super user only access for SCSI passthru. • Fixes a cluster problem where opening a file after open/close of its clone deadlocks the AdvFS thread. • Adds unified wait support in conjunction with clustered RDG multichannel wait flag fix to allow for more efficient processing by Oracle processes. • Fixes a problem where network interfaces can appear unresponsive to network traffic. • Corrects a CFS problem where the data on an AdvFS clone fileset may get overwritten as an unexpected side effect of using directio. The problem occurs when the program issuing the directio open is running on a CFS client AND the fileset involved has been cloned AND a rewrite occurs involving pages not yet modified since the creation of the clone. • Fixes mbuf memory corruption when using ICS/TCP. • Fixes a problem with vm_faults against anon objects mapped by multiple map entries. • Corrects the problem of a thread deadlocking against itself under the following conditions: – Running in a cluster. – Opening (and then closing) a directory that has an index file. – Trying to open the index file through .tags (for example, defragment does that) and by coincidence getting the vnode that pointed to the directory that the index file is attached to. • Fixes a performance problem and the results are large performance increases in configurations where more than 8 tapes are supported on a FibreChannel (usually behind an MDR or FCTCII).

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

Patch 647.00 continued	• Fixes a problem in kernel threads where multi-threaded applications were allowed to start running prior to virtual memory mapping swapin. This was prevented by adding a flag to mark when the map is swapped out and no thread swapins can occur until this flag is cleared. • Fixes a problem in the Virtual Memory subsystem where a process hangs and cannot be killed. This problem only happens on NUMA systems. • Contains fixes that ensure FibreChannel system configurations can properly identify boot and swap devices required to obtain crash dumps. This patch requires that FibreChannel systems which utilize FibreChannel devices for boot and swap be properly configured. • Fixes a panic of "malloc_leak: free with wrong type" when using kmem-debug-protect. • Fixes an issue where Sybase reports "Error: 1613" and "host process disconnected" errors. • A threaded section of application code can crash when using granularity hints (GH). • Ensures that certain invariants within the kernel concerning clone maps are maintained. It maintains consistency and correctness of the clone maps. • Fixes a problem that can cause a "kernel memory fault" panic in load_from_shadow_rec(). • Fixes incorrect usage of UNMOUNT_TRY_READ in AutoFS. • Fixes a bug that can cause a panic when a system is powering down. • Fixes the following problems using hwmgr command: KMF FTX_DONE_URDR: BAD FTX UNALIGNED KERNEL SPACE ACCESS FROM KERNEL MODE KMF FROM HWC_LOOKUP_DEVT_SAFE HWCC_JACKET_RTN: BAD CALL TO KCH HWCC_EVAL_REQUEST: INFALLIBLE PROPOSAL RETURNED ERROR HWCC_JACKET_RTN: INFALLIBLE PROPOSAL RETURNED ERROR • Prevents lock hierarchy violations due to putpage/migrate interaction.

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

Patch 647.00 continued	• Fixes a problem where an AdvFS direct I/O read can cause a "kernel memory fault" system panic. The problem occurs when the following two conditions are met: – One of the pages cannot be read. – The I/O request is not an even multiple of 512 bytes. • Allows POSIX semaphores/msg queues to operate properly on a CFS client. • Fixes a problem in which issuing a quot -h command causes a memory fault when the /etc/fstab file contains a mount point that is not mounted. • Fixes a system panic with panic string: "lock_terminate: lock held". This is being caused by the table call which, when accessing an open file table from another task, was not doing the proper locking. • A potential security vulnerability has been discovered in networking where, under certain circumstances, a remote system can take over packets destined for another host. • Fixes a problem where the UBC subsystem fails to purge pages because of bound purge_thread. • Fixes the following system panics: Kernel Memory Fault in function sth_close_fifo() when closing a vnode that belongs to a FIFO simple_lock: time limit exceeded in spec_reclaim • Fixes a problem in which a TCP socket can continue to receive data with no application running. • Corrects a problem where the network subsystem sometimes sends a null TCP packet when a connection is reset. • A check for managed address may return an invalid value when called with the address of a gh region not on rad 0. • Fixes a kernel panic with "xfer_hole_stg: unaligned kernel access" or "xfer_hole_stg: kernel memory fault" messages.
Patch 649.00 OSF510-261	**Pathc:** Possible hang occurs with libaio and libaio_raw **State:** New This patch warns a user of a possible hang that can occur when a program is linked to both libaio and libaio_raw.

3

Summary of TruCluster Software Patches

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

Table 3–1 lists patches that have been updated.

Table 3–2 provides a summary of patches in Patch Kit-0004.

Table 3–1: Updated TruCluster Software Patches

Patch IDs	Change Summary
Patches 66.00, 80.00	New
Patches 17.00, 42.00, 43.00	Superseded by Patch 45.00
Patches 28.00, 41.00, 46.00, 47.00	Superseded by Patch 49.00
Patches 11.00, 30.0, 67.00	Superseded by Patch 69.00
Patches 5.00, 7.00, 32.00, 70.00	Superseded by Patch 72.00
Patches 15.00, 33.00, 34.00, 35.00, 36.00, 37.00, 39.00, 73.00, 74.00, 75.00	Superseded by Patch 77.00
Patch 78.00	Superseded by Patch 80.00
Patches 2.00, 13.00, 18.00, 19.00, 20.00, 21.00, 22.00, 23.00, 24.00, 26.00, 50.00, 51.00, 52.00, 53.00, 54.00, 55.00, 56.00, 57.00, 58.00, 59.00, 60.00, 61.00, 62.00, 64.00	Superseded by Patch 82.00

Table 3–2: Summary of TruCluster Patches

Patch IDs	Abstract
Patch 4.00 TCR510DX-001	**Patch:** Fix for Cluster Alias Manager system management tool **State:** Existing This patch fixes the Cluster Alias Manager system management tool from crashing and displaying errors.
Patch 9.00 TCR510-001	**Patch:** Initializing the MC-API results in system crash **State:** Existing This patch fixes a problem where on the AlphaServer GS160 systems, initializing the MC-API results in the system crashing with a "kernel memory fault" message.

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

Patch 45.00 TCR510-043	**Patch:** Prevents ics_mct error panic on clusters **State:** Supersedes patches TCR510-018 (17.00), TCR510-028 (42.00), TCR510-052 (43.00) This patch corrects the following: • Eliminates unnecessary rail failovers in vhub configurations and removes rmerror_int diagnostic messages. • Fixes an issue which causes all cluster nodes to hang or panic if a Wildfire is halted via the halt button. • Fixes a panic that is caused in a clustered environment that has the following error message: rm_request_on_bad_prail • Prevents an "ics_mct: Error from establish_RM_notification_channel" panic on clusters.
Patch 49.00 TCR510-037	**Patch:** Fixes networking issues within cluster environment **State:** Supersedes patches TCR510-019 (28.00), TCR510-029 (41.00), TCR510-041 (46.00), TCR510-048 (47.00) This patch corrects the following: • Fixes the cluamgr command where it will display the alias status even if no cluster member has joined the alias. • Fixes a problem in which RPC requests to the cluster alias may fail with "RPC timeout" message. • Fixes a cluster node hang from in_pcbnotify. • Fixes a problem that a rebooted node not able of sending messages to the cluster alias. • Fixes multiple networking issues within a cluster environment: • Cluster member loses connectivity with clients on remote subnets. • aliasd not handling multiple virtual aliases in a subnet and/or IP aliases. • Allows cluster members to route for an alias without joining it. • aliasd writing illegal configurations into gated.conf.memebrX. • Default route not being restored after network connectivity issues. • Fixes a race condition between aliasd and gated. • Fixes a problem with a hang caused by an incorrect /etc/hosts entry.
Patch 66.00 TCR510-027	**Patch:** CAA unable to update the state of devices **State:** New This patch is for systems running TruCluster Server V5.1 with the following configurations: • Tapes and/or media changer devices used as CAA resources. • A combination of tapes, media changers, and network interfaces used as CAA resources. The patch fixes a problem that prevents CAA from updating the state of any of the above resources when connectivity to the corresponding device (tape, media changer, or network) is lost or restored.

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

Patch 69.00 TCR510-049	**Patch:** Fix for KMF with RDG autowiring mechanism **State:** Supersedes patches TCR510-007 (11.00), TCR510-024 (30.00), TCR510-036 (67.00) This patch corrects the following: • Corrects a problem in which the RDG subsystem will stop sending messages even though there are messages which are deliverable. • Fixes an incorrect display of the following warning message at boot time: rdg: failed to start context rcvq scan thread • Fixes a kernel memory fault with the RDG autowiring mechanism, also seen as a “pte not valid” crash. • Adds a multichannel wait flag to pid_unblock. • Contains performance enhancements. • Fixes a problem with RDG whereby broadcast packets can interact with the context receive queue.
Patch 72.00 TCR510-039	**Patch:** Fixes a panic that causes a CNX QDISK error message **State:** Supersedes patches TCR510-002 (5.00), TCR510-003 (7.00), TCR510-023 (32.00), TCR510-042 (70.00) This patch corrects the following: • Fixes an occasional cluster hang which can occur after a Memory Channel error. • Fixes a kernel memory fault which occurs in the ics_mct_ring_recv() routine. The kernel memory fault is seen when a node is booting into the cluster, and can occur on the booting node or on another node. • Fixes a problem in ICS where ring_recv() does not properly handle a change in channel numbers. The fix will, in turn, improve validation of the connection structure on node joins. • Fixes the way communication errors occur on clusters such that a down node will not declare all other nodes dead. • Fixes the problem that causes a panic with error message "CNX QDISK: Yielding to foreign owner with quorum" caused by a long running thread, ICS/MCT receive thread, which defers other kernel threads from accessing the CPU.

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

Patch 77.00 TCR510-034	**Patch:** Fixes KZPCC controller problem **State:** Supersedes patches TCR510-005 (15.00), TCR510-021 (33.00), TCR510-009 (34.00), TCR510-016 (35.00), TCR510-011 (36.00), TCR510-022 (37.00), TCR510-012 (39.00), TCR510-035 (73.00), TCR510-038 (74.00), TCR510-030 (75.00) This patch corrects the following: • Fixes two TruCluster problems: – If a Quorum disk is manually added by the command clu_quorum -d add, the disk becomes inaccessible because the PR flag is not being cleaned up. The same command will work in the next reboot. – A cluster member cannot boot under a specific hardware setup. The CFS mount fails because of the PR flag is not cleaned up. • Addresses the need for IOCTL for remote DRD, adds clean up for failed remote closes for non-disks, fixes error returns on failed tape/changer closes, and fixes tape deadlock experienced in netbackups. • Fixes an issue with a tape/changer failing to correctly report a close failure of a device in a cluster environment. • Fixes a problem which results in a system panic while doing tape failovers. • Fixes a node panic during fiber port disables. • Fixes an issue with a tape/changer giving back “busy on open” if a close from a remote node failed. • Provides the TCR portion of the functionality to support EMC storage boxes that support Persistent Reserves (SCSI command set) as defined by the final SCSI specification. • Fixes an issue with requests being stuck on a failed disk in a cluster. • Allows high density tape drives to use the high density compression setting in a cluster environment. • Fixes a kernel memory fault panic that can occur within a cluster member during failover while using shared served devices. • Aixes an issue with the hwmgr -delete command that causes a panic in a cluster. • Fixes the KZPCC controller problem seen when deleting a Virtual Drive using SWCC and adding the same drive back can result in the disk being unaccessible.
Patch 80.00 TCR510-047	**Patch:** Fixes an Oracle process hang **State:** Supersedes patch TCR510-033 (78.00) This patch corrects the following: • Fixes an Oracle process hang if a node fails after receiving a rsbinfo message. • Fixes a DLM problem where two processes could take out the same lock.

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

Patch 82.00 TCR510-064	**Patch:** TCR510-058 **State:** Supersedes patches TCR510-004 (2.00), TCR510-006 (13.00), TCR510-026 (18.00), TCR510-020 (19.00), TCR510-013 (20.00), TCR510-015 (21.00), TCR510-017 (22.00), TCR510-014 (23.00), TCR510-025 (24.00), TCR510-008 (26.00), TCR510-056 (50.00), TCR510-050 (51.00), TCR510-054 (52.00), TCR510-057 (53.00), TCR510-046 (54.00), TCR510-040 (55.00), TCR510-031 (56.00), TCR510-032 (57.00), TCR510-051 (58.00), TCR510-060 (59.00), TCR510-044 (60.00), TCR510-053 (61.00), TCR510-045 (62.00), TCR510-058 (64.00) 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. • Provides a small TPC-C performance optimization to cfsspec_read for reporting TPC-C single node cluster numbers. • When attempting to roll a patch kit on a single member cluster without this patch, the following error messages will be seen when running the postinstall stage: *** Error*** Members '2' is NOT at the new base software version. *** Error*** Members '2' is NOT at the new TruCluster software version. • During backup stage of clu_upgrade setup 1, clu_upgrade is unable to determine the name of the kernel configuration file. • clu_upgrade does not check the availabilty of space in /, /usr, and /usr/i18n. • During the preinstalled phase, clu_upgrade will ignore a no answer when the user is prompted, during an error condition, whether they wish to continue. • clu_upgrade incorrectly assumes that if the directory /usr/i18n exists, then it is in its own file system. • After the clu_upgrade clean phase, the final step of clu_upgrade, no message is displayed that leads the user to believe they have completed the upgrade. Only the prompt is returned and the clu _upgrade -completed clean command reports that the clean had not completed. • clu_upgrade can display "Could not get property..." and "...does not exist" type of error messages during the undo install phase. • The clu_upgrade undo switch command, after completing a clu_upgrade switch command, should display an error message instead of claiming it has succeeded. • Fixes a problem with disaster recovery whereby the node being restored will hang on boot. • Corrects a problem in which a cluster may panic with a "cfsdb_assert" message when restoring files from backup while simultaneously relocating the CFS server for that file system. • Corrects a problem in which a cluster member can panic with the panic string "cfsdb_assert" when a NFS v3 TCP client attempts to create a socket using mknod(2). • Corrects a problem in which a cluster member will panic with the patch string "lock_terminate: lock held" from cinactive().

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

Patch 82.00 continued	• Fixes a hang seen while running collect and the vdump utility. This patch prevents the hang in tok_wait from occurring. This also prevents a cfsdb_assert panic that contains the following message: Assert Failed: (tcbp->tcb_flags & TOK_GIVEBACK) == 0 • Prevents a cfsdb_assert panic from occurring in the cfs block reserve code. The system is most likely running process accounting that will receive this type of panic. • Provides performance enhancements for copying large files (files smaller than the total size of client's physical memory) between a CFS client and server within the cluster. • Corrects a token hang situation by comparing against the correct revision mode. • Fixes a bug in the cluster filesytem that can cause a kernel memory fault. • Eliminates superfluous AutoFS auto-mount attempts during rolling upgrade. These attempted auto-mounts slow down certain operations and leave the AutoFS namespace polluted with directories prefexed with ".Old..". • Fixes memory leak in cfscall_ioctl(). • Fixes a panic with the following error message: panic: cfsdb_assert • Contains corrections required for proper operation of Oracle 9i with Tru64 UNIX/TruCluster 5.1. The problems corrected include: – Processes hanging when using Cluster File System/Direct I/O feature. – Improper handling of direct I/O to an AdvFS fileset if a clone fileset was already in use, potentially resulting in an inconsistent backup. – Using ls -l, the Cluster File System file attribute could be seen inconsistently from the server and client members. For example, a file's mode could be seen differently from the server and the client. – A file opened for Direct I/O on the Cluster File System server may inappropriately be opened in non-direct I/O mode by a client. – Oracle processes hanging due to shutting down one cluster member. – A problem with the Cluster File System which could cause a cluster system to panic with the panic string "kernel memory fault" in the routine mc_bcopy(). – A problem with Cluster File System which could cause a cluster member to panic with the panic string "uiomove: mode." This problem could cause Oracle multi-instance data bases to crash with the message similar to the following: ORA-27063: skgfospo: number of bytes read/written is incorrect

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

Patch 82.00 continued	• Fixes data inconsistency problems that can be seen on clusters that are NFS clients. • Frevents a cfsdb_assert panic from occurring in cfs_reclaim. This panic has been seen while running ensight7. • Prevents a potential hang due to external NFS servers. • Provides a warning to users installing a patch kit that includes a patch which requires a version switch. The warning informs the user that the installed patches include a version switch which cannot be removed using the normal patch removal procedure. The warning allows the user to continue with the switch stage or exit clu_upgrade. • Prevents a potential hang that can occur on a CFS failover. • Allows POSIX semaphores/msg queues to operate properly on a CFS client. • Allows the command cfsstat -i to execute properly. • Corrects a problem which can cause cluster members to hang, waiting for the update daemon to flush /var/adm/pacct. • Fixes a potential CFS hang on defragment.