

# Tru64 UNIX 5.1 and TruCluster Server 5.1

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

---

**April 2001**

This manual describes the release notes and contents of Patch Kit-0003. 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*.

---

© 2001 Compaq Computer Corporation

© 2001 Compaq Computer Corporation

COMPAQ, the Compaq logo, AlphaServer, TruCluster, ULTRIX, and VAX Registered in U.S. Patent and Trademark Office. Alpha and Tru64 are trademarks of Compaq Information Technologies Group, L.P.

Motif, OSF/1, UNIX, X/Open, and The Open Group are trademarks of The Open Group.

All other product names mentioned herein may be trademarks or registered trademarks of their respective companies.

Confidential computer software. Valid license from Compaq required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Compaq shall not be liable for technical or editorial errors or omissions contained herein. The information in this document is provided "as is" without warranty of any kind and is subject to change without notice. The warranties for Compaq products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.

---

# Contents

## About This Manual

### 1 Release Notes

1.1	Patch Process Resources .....	1-1
1.2	Required Storage Space .....	1-1
1.3	Difference Between the First and Second Release Version 5.1 Kits ..	1-2
1.3.1	Installing Kit-0003 for the First Time .....	1-2
1.3.2	Installing the Second Release of Kit-0003 over the First Release of Kit-0003 .....	1-3
1.4	Release Note for Tru64 UNIX Patch 399.00 .....	1-4
1.4.1	AdvFS and Direct I/O .....	1-4
1.4.2	Technical Update for KZPCC products .....	1-5
1.4.3	Release Note for KZPCC Products .....	1-6
1.4.4	Problem with Multi-user Mode Application .....	1-6
1.4.5	New Graphics Card .....	1-6
1.4.6	DEGPA-TA Gigabit Ethernet Device .....	1-8
1.5	Release Note for Tru64 UNIX Patch 287.00 .....	1-9
1.6	Release Note for Tru64 UNIX Patch 371.00 .....	1-9
1.7	Release Note for TruCluster Server Software .....	1-9
1.8	Release Note for Broken Link Problem .....	1-9
1.9	Release Note for Potential Rolling Upgrade Problem .....	1-10
1.10	Release Note for Tru64 UNIX Patch 169.00 .....	1-11
1.11	Release Note for Tru64 UNIX Patch 270.00 .....	1-12

### 2 Summary of Base Operating System Patches

### 3 Summary of TruCluster Software Patches

#### Tables

2-1	Updated Base Operating System Patches .....	2-1
2-2	Summary of Base Operating System Patches .....	2-3
3-1	Updated TruCluster Software Patches .....	3-1
3-2	Summary of TruCluster Patches .....	3-1



---

# About This Manual

This manual contains information specific to Patch Kit-0003 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.

---

## 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-0003.

### 1.1 Patch Process Resources

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

- To obtain the latest patch kit for your operating system and cluster:  
`http://ftp1.support.compaq.com/public/unix/`
- To view or print the latest 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 ~66.2 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 ~67 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 ~616 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 ~50 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 ~51 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 ~675 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.

## 1.3 Difference Between the First and Second Release Version 5.1 Kits

The Version 5.1 Patch Kit-0003 was re-issued to correct a problem with the baselining operation of the patch installation utility, `dupatch`. The patches themselves are exactly the same in both kits. You can tell the difference between these kits as follows:

- The file for the initial kit (which has been recalled) is `T64V51AS0003-20010413.tar`. When installed, the `dupatch` utility revision in this kit is listed as Rev. 28-03.
- The file for the second release of this kit is `T64V51AS0003-20010521.tar`. When installed, the `dupatch` revision in this kit is listed as Rev. 29-02.

To install this patch kit, use one of the following procedures.

### 1.3.1 Installing Kit-0003 for the First Time

If you are installing the second release of Patch Kit-0003 and did not install the initial release of Patch Kit-0003, you need only follow the instructions in the



*Patch Kit Installation Instructions* document provided with your kit. No special action is needed.

### 1.3.2 Installing the Second Release of Kit-0003 over the First Release of Kit-0003

If you previously installed the initial release of Patch Kit-0003 on a system, the steps you take with the second release kit depend on whether or not your system contains manually installed customer-specific patches (CSPs):

- In systems without CSPs or with CSPs that were installed with the `dupatch` utility, you need only re-install the patch installation tools.
- In systems with manually installed CSPs, you need to perform the baselining procedure and then re-install the patches.

The following sections describe these procedures. Compaq recommends that you have the *Patch Kit Installation Instructions* available.

#### Common Steps

The following steps are common to all stand-alone and clustered systems:

1. From root, extract the `T64V51AS0003-20010521.tar` file to a locally mounted file system. For example:

```
# script untar.log
# tar -xpvf T64V51AS0003-20010521.tar
```

2. From the directory containing the extracted files run `dupatch`:

```
# ./dupatch
```

---

#### Note

---

Do not run the version of `dupatch` in `/usr/sbin`.

---

3. When the `dupatch` menu is displayed, verify that the revision is listed as `Rev. 29-02`.

If your system has no customer-specific patches installed, type `q` to exit `dupatch`; you have done all you need to do. For systems containing CSPs, see the next section.

---

#### Note

---

If you want to install the new installation tools without invoking the `dupatch` menu (for example, if you are using a script), use the following command. You will, however, need to invoke the `dupatch` menu if you want to verify the `dupatch` revision.

```
dupatch -track -kit patch_kit -type kit
```

---

#### Additional Steps for Manually Installed CSPs

If your system contains manually installed customer-specific patches, perform the previous steps, and then do the following:

4. Review your session logs from the installation of the initial Patch Kit-0003 to determine if any critical patches failed to install. If you find none, you do not have to do anything else. If you find critical patches that failed to install, continue with the following steps.

5. Run the baseline option. See the *Patch Kit Installation Instructions* for step-by-step instructions on baselining.
6. Install the patch kit.

---

**Note**

---

If you are installing the patch kit on a cluster using the Rolling Upgrade procedure, perform steps 1 through 5 before beginning the Rolling Upgrade.

Perform step 6 during the Install Stage of the Rolling Upgrade procedure. See the *Patch Kit Installation Instructions* for step-by-step instructions on performing a Rolling Upgrade.

---

## 1.4 Release Note for Tru64 UNIX Patch 399.00

### 1.4.1 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_dbl.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
***
```

## 1.4.2 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.

### 1.4.3 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 inaccessible. Even though the `hwmgrr` sees the drive being deleted and added back, it can not be diskabeled 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.

### 1.4.4 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 399.00 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.

### 1.4.5 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 287.00, 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.

#### 1.4.6 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.

## 1.5 Release Note for Tru64 UNIX Patch 287.00

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 399.00, 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>

## 1.6 Release Note for Tru64 UNIX Patch 371.00

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>

## 1.7 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.

## 1.8 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
```

## 1.9 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/.smbd`. 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/.smbd./OSFPAT00018600505.inv
grep: can't open ./usr/.smbd./OSFPAT00019200505.inv
grep: can't open ./usr/.smbd./OSFPAT00020500505.inv
grep: can't open ./usr/.smbd./OSFPAT00021100505.inv
grep: can't open ./usr/.smbd./OSFPAT00016500505.inv
grep: can't open ./usr/.smbd./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:  

```
# bckckrc
```

  

```
# 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.

## 1.10 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`.

## 1.11 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. (Note: 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>

---



## Summary of Base Operating System Patches

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

Table 2–1 lists patches that have been updated.

Table 2–2 provides a summary of patches.

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

Patch IDs	Change Summary
Patches 171.00, 173.00, 226.00, 249.00, 252.00, 255.00, 278.00, 283.00, 285.00, 290.00, 292.00, 294.00, 300.00, 302.00, 304.00, 306.00, 308.00, 310.00, 312.00, 314.00, 316.00, 318.00, 320.00, 262.00, 326.00, 328.00, 226.00, 333.00, 335.00, 337.00, 339.00, 341.00, 343.00, 345.00, 347.00, 349.00, 351.00, 353.00, 362.00, 360.00, 364.00, 366.00, 296.00, 368.00, 372.00, 374.00, 376.00, 378.00, 232.00, 381.00, 385.00, 387.00, 389.00, 324.00, 395.00, 401.00, 403.00, 405.00	New
Patch 13.00	Superseded by Patch 175.00
Patches 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	Superseded by Patch 399.00
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, 240.00, 241.00	Superseded by Patch 243.00
Patch 9.00	Superseded by Patch 245.00
Patches 246.00, 247.00	Superseded by Patch 249.00
Patch 250.00	Superseded by Patch 252.00
Patch 253.00	Superseded by Patch 255.00
Patches 34.00, 227.00, 228.00	Superseded by Patch 230.00
Patches 64.00, 256.00, 257.00, 258.00	Superseded by Patch 260.00
Patches 55.00, 266.00	Superseded by Patch 268.00
Patch 44.00	Superseded by Patch 270.00
Patch 70.00	Superseded by Patch 280.00
Patch 281.00	Superseded by Patch 283.00
Patch 119.00	Superseded by Patch 287.00
Patch 288.00	Superseded by Patch 290.00
Patches 78.00, 263.00	Superseded by Patch 265.00

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

Patch 128.00	Superseded by Patch 298.00
Patch 66.00	Superseded by Patch 322.00
Patch 132.00	Superseded by Patch 330.00
Patches 72.00, 354.00, 355.00, 356.00	Superseded by Patch 358.00
Patches 145.00, 146.00, 148.00	Superseded by Patch 370.00
Patch 381.00	Superseded by Patch 379.00
Patch 84.00	Superseded by Patch 391.00
Patch 160.00	Superseded by Patch 393.00

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

Patch IDs	Abstract
Patch 7.00 OSF510-037B	<b>Patch:</b> Threaded programs do not terminate <b>State:</b> Existing This patch fixes hangs in threaded programs with subprocesses created with <code>nfork(NULL)</code> . Examining one of the hanging subprocesses shows that it has called <code>fopen()</code> and is waiting for the <code>jobptr</code> mutex in <code>_findiop()</code> .
Patch 15.00 OSF510-009A	<b>Patch:</b> libst shared library fix <b>State:</b> Existing This patch fixes a problem with two routines in the libst library, <code>st_obj_open()</code> and <code>st_obj_write()</code> . 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	<b>Patch:</b> libst static library fix <b>State:</b> Existing This patch fixes a problem with two routines in the libst library, <code>st_obj_open()</code> and <code>st_obj_write()</code> . 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	<b>Patch:</b> Fix for booting problem via network interface <b>State:</b> 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 21.00 OSF510-020	<b>Patch:</b> Corrects a stack overflow panic <b>State:</b> Existing This patch corrects a stack overflow panic encountered during the startup of the system management daemon ( <code>smsd</code> ) on configurations with more than 255 devices.
Patch 38.00 OSF510-021	<b>Patch:</b> Fix for panic that occurs when <code>kloadsrv</code> is restarted <b>State:</b> Existing This patch fixes a system panic that may occur when <code>/sbin/kloadsrv</code> is restarted.
Patch 40.00 OSF510X11-001	<b>Patch:</b> Fix for <code>lbxproxy</code> utility <b>State:</b> Existing This patch fixes a problem where the X windows <code>lbxproxy</code> utility, which is used to make Low Bandwidth X (LBX) connections to an X server, did not accept local connections.
Patch 42.00 OSF510-031	<b>Patch:</b> Fix for <code>grep</code> command <b>State:</b> Existing This patch fixes a problem with the <code>grep</code> command in which the options <code>-p -v</code> together do not produce any output.
Patch 49.00 OSF510-024	<b>Patch:</b> Fixes the processing of export lists <b>State:</b> Existing This patch fixes the processing of export lists with a <code>/</code> (slash) in them.
Patch 51.00 OSF510-043	<b>Patch:</b> Change to <code>kloadsrv</code> and <code>hotswapd</code> entries <b>State:</b> Existing This patch changes the <code>kloadsrv</code> and <code>hotswapd</code> entries in the <code>/etc/inittab</code> file. The change will prevent possible problems with dynamically loaded kernel modules when shutting down to single user mode.

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

Patch 57.00 OSF510-041	<b>Patch:</b> Fix for panic or system hang that may occur on DS20E <b>State:</b> Existing This patch 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.
Patch 59.00 OSF510-025	<b>Patch:</b> Fix for tagged-file induced automount requests <b>State:</b> Existing This patch avoids tagged-file induced automount requests in AutoFS.
Patch 68.00 OSF510-003	<b>Patch:</b> Fix for dump command <b>State:</b> Existing The patch fixes a problem where a user could not dump to a regular file.
Patch 74.00 OSF510-018	<b>Patch:</b> Fixes environmental warning in GS systems <b>State:</b> 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	<b>Patch:</b> Hardware manager inaccurately reports the CPU speed <b>State:</b> 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.
Patch 82.00 OSF510CDE-001	<b>Patch:</b> List of application groups is not re-created <b>State:</b> 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 92.00 OSF510-069	<b>Patch:</b> Fix for system hang during a route command <b>State:</b> New This patch fixes a network problem where a system can hang during a route command.
Patch 105.00 OSF510-017	<b>Patch:</b> Prevents not currently mounted warning messages <b>State:</b> 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	<b>Patch:</b> Fix for tcl <b>State:</b> 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.



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

---

Patch 109.00 OSF510-085	<b>Patch:</b> bextract does not create device special files <b>State:</b> New. Supersedes patches OSF510-045 (45.00), OSF510-029 (47.00) This patch corrects the following: <ul style="list-style-type: none"><li>• Adjusts the sleep time for slower robot tape changers to allow them time to replace a tape.</li><li>• Fixes a kernel panic caused by btcreate when it generated scripts to recreate LSM volumes on restore operations.</li><li>• Fixes a problem where the device special files are not being created by bextract.</li></ul>
Patch 111.00 OSF510DX-003	<b>Patch:</b> Fix for smsd crash <b>State:</b> 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	<b>Patch:</b> Fix for Xt <b>State:</b> New. Supersedes patch OSF510X11-005A (112.00) This patch corrects the following: <ul style="list-style-type: none"><li>• 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.</li><li>• Fixes the problem of XmStringGetLtoR() failing in dxhanziim when it runs in a C/en_US.ISO8859-1 locale.</li></ul>
Patch 117.00 OSF510X11-009B	<b>Patch:</b> Fixes a memory leak in Xt <b>State:</b> New. Supersedes patch OSF510X11-005B (115.00) This patch corrects the following: <ul style="list-style-type: none"><li>• 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.</li><li>• Fixes the problem of XmStringGetLtoR() failing in dxhanziim when it runs in a C/en_US.ISO8859-1 locale.</li></ul>
Patch 121.00 OSF510CDE-002	<b>Patch:</b> Fix for dtlogin <b>State:</b> 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.

---

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

---

Patch 124.00 OSF510DX-006	<p><b>Patch:</b> Message fragments now I18N compatible</p> <p><b>State:</b> Supersedes patches OSF510DX-002 (36.00), OSF510DX-005 (122.00)</p> <p>This patch fixes the following dxaccounts problems:</p> <ul style="list-style-type: none"><li>• A system running ASU experiences a dxaccounts crash problem when a user is deleted from PC User view.</li><li>• The dxaccounts dialog messages are incorrectly displayed when a user is added with no password entry.</li><li>• The dxaccounts utility is unable to create a new user from the PC Users view on a system with ASU installed.</li><li>• The following problems can occur with the dxaccounts application on ASU system:<ul style="list-style-type: none"><li>– The dxaccounts utility crashes when the root icon is double clicked.</li><li>– The full name of a new PC account is not mapped to a UNIX user.</li><li>– Erasing a PC account’s fields does not work; the values erased remain.</li><li>– The default values of Home Directory, Login Script, and User Profile Path for a PC user are invalid.</li></ul></li><li>• Changing root’s login/uid is enabled via cli/dxaccounts utilities.</li><li>• Incorrect results of usermod -G.</li><li>• The -x account_inactive   account_expiration options do not set the attributes.</li><li>• 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.</li><li>• Fixes message fragments to make them I18N compatible.</li></ul>
Patch 126.00 OSF510-056	<p><b>Patch:</b> Fix for kernel stack not valid halt</p> <p><b>State:</b> New</p> <p>When the user runs ATM Lan Emulation, using more than four ATM NetRAIN interfaces can result in recursive calls causing a “kernel stack not valid” halt.</p>
Patch 130.00 OSF510-067	<p><b>Patch:</b> Fix for lock hierarchy violation panic</p> <p><b>State:</b> New. Supersedes patch OSF510-034 (80.00)</p> <p>This patch corrects the following:</p> <ul style="list-style-type: none"><li>• 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.</li><li>• 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.</li></ul>
Patch 134.00 OSF510-026	<p><b>Patch:</b> Fix for collect command</p> <p><b>State:</b> New</p> <p>This patch fixes several problems with the collect command. It adds sysloging when collect suspends, resumes, or receives a signal.</p>

---

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

---

Patch 137.00 OSF510X11-008A	<b>Patch:</b> Fix for Xlib memory leak <b>State:</b> New. Supersedes patch OSF510X11-004A (135.00) This patch corrects the following: <ul style="list-style-type: none"><li>• 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.</li><li>• Provides enhanced support for UTF-8 and UCS-4 locales.</li></ul>
Patch 140.00 OSF510X11-008B	<b>Patch:</b> Support for UTF-8 and UCS-4 locales <b>State:</b> New. Supersedes patch OSF510X11-004B (138.00) This patch corrects the following: <ul style="list-style-type: none"><li>• 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.</li><li>• Provides enhanced support for UTF-8 and UCS-4 locales.</li></ul>
Patch 142.00 OSF510X11-006A	<b>Patch:</b> Fixes memory leaks in Motif library <b>State:</b> 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 144.00 OSF510X11-006B	<b>Patch:</b> Fix for libXm <b>State:</b> 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	<b>Patch:</b> Fix for advscan <b>State:</b> New This patch fixes a problem where advscan -a -g does not display bootable partitions properly.
Patch 158.00 OSF510CDE-003	<b>Patch:</b> Fix for dtmail problem <b>State:</b> 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	<b>Patch:</b> Fix for diskconfig error message <b>State:</b> 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	<b>Patch:</b> Fix for bttape <b>State:</b> New bttape now uses the lock file /usr/run/bttape.pid for checking multiple instances. Also, the default addlist and fslis are created appropriately.
Patch 171.00 OSF510-098	<b>Patch:</b> Fix for voldctl stop command <b>State:</b> New This patch corrects the voldctl stop command behaviour for cluster support.
Patch 173.00 OSF510-057	<b>Patch:</b> fixso command causes segmentation fault <b>State:</b> New This patch fixes a problem with the /usr/ucb/fixso command that can cause a segmentation fault.

---

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

---

Patch 175.00 OSF510-161	<p><b>Patch:</b> Fix for vrestore problems</p> <p><b>State:</b> Supersedes patch OSF510-013 (13.00)</p> <p>This patch fixes the following problems:</p> <ul style="list-style-type: none"><li>• A previous patch caused incomplete restores.</li><li>• 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.</li><li>• A warning message is displayed and vrestore aborts if it fails to malloc space for a property list.</li><li>• A message which had been inserted at the end of the message file had the wrong message category (this could cause messaging confusion).</li><li>• 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.</li><li>• Corrupted property list information could cause an infinite loop.</li><li>• Fixes problems in the vdump command:<ul style="list-style-type: none"><li>– Failed to flag compressed extended attributes records that are split across a vdump BLOCK boundary.</li><li>– 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.)</li><li>– Corrects "Rewinding" message to avoid a segfault with Internationalized messages.</li></ul></li><li>• Fixes problems in the vrestore command<ul style="list-style-type: none"><li>– 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".</li><li>– 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".</li><li>– 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).</li><li>– 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).</li></ul></li></ul>
Patch 226.00 OSF510-107B	<p><b>Patch:</b> Fix for delayed AdvFS requests</p> <p><b>State:</b> New</p> <p>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.</p>

---

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

---

Patch 230.00 OSF510-109B	<p><b>Patch:</b> Fix for POSIX Threads Library</p> <p><b>State:</b> Supersedes patches OSF510-039B (34.00), OSF510-212B (227.00), OSF510-206B (228.00)</p> <p>This patch fixes problems for threaded applications running on Tru64 UNIX V5.1:</p> <ul style="list-style-type: none"><li>• 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.</li><li>• 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.</li><li>• 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.</li></ul>
Patch 232.00 OSF510-158B	<p><b>Patch:</b> Adds support for activating temporary data logging</p> <p><b>State:</b> New</p> <p>This patch provides support for activating temporary data logging on a mount point.</p>
Patch 243.00 OSF510-150	<p><b>Patch:</b> Security (SSRT0689U)</p> <p><b>State:</b> 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)</p> <p>This patch corrects the following problems:</p> <ul style="list-style-type: none"><li>• Fixes a problem of the getaddrinfo() library call returning a failing status.</li><li>• Increases the number of places of precision for formatted printing of long doubles.</li><li>• 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).</li><li>• 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 jobptr mutex in _findiop().</li><li>• Fixes the printing of 0.0 when precision is specified for a %g type conversion.</li><li>• 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().</li><li>• 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.</li></ul>

---

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

---

Patch 243.00 continued	<ul style="list-style-type: none"><li>• 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 <code>__sbrk_override</code> malloc tuning variable is set which caused malloc to try to allocate too much memory.</li><li>• Fixes a problem with the <code>mallinfo()</code> call which can cause an application to fail if run on a RAD other than 0.</li><li>• fixes a problem with the <code>mallinfo()</code> call which can cause an application to fail if run on a RAD other than '0'.</li><li>• Restores correct behavior that existed on pre-V5.0 releases for <code>ecvt()</code> and <code>fcvt()</code>. Floating point exceptions and core dumps no longer occur when denormalized values are passed to <code>ecvt()</code> and <code>fcvt()</code>.</li><li>• Resolves issues with customer applications that experienced floating point exceptions and core dumps when passing denormalized values to <code>ecvt()</code> and <code>fcvt()</code> that subsequently caused INFORMIX databases to crash.</li><li>• Fixes the return values for <code>vwprintf()</code> functionality when used with wide characters.</li><li>• Increases the input buffer size limits for the <code>scanf</code> family of functions to the MAXINT input buffer size.</li><li>• Fixes the problem of optimized programs printing incorrect values for long doubles.</li><li>• Adds logic that implements maximum size checks for input width descriptors on numeric <code>scanf()</code> format elements.</li><li>• Corrects a regular expression performance problem in <code>libc</code>.</li><li>• Fixes a potential online help build problem when <code>dthelptag</code> is used to compile online help files in a multibyte locale.</li><li>• Fixes regular expression handling with non-default locale settings.</li></ul>
Patch 245.00 OSF510-198	<p><b>Patch:</b> Install does not allow subset name with an underscore</p> <p><b>State:</b> New. Supersedes patch OSF510-046 (9.00)</p> <p>This patch fixes the following problems:</p> <ul style="list-style-type: none"><li>• 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, <code>MQS_HTML_PUBS</code>.</li><li>• Fixes a problem with the deletion process on a cluster system when a member node is running <code>/usr/bin/csh</code>. The process fails with a command not found error.</li><li>• Fixes a problem with the deletion process not terminating when the C DELETE phase of the subset control program fails.</li></ul>

---

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

---

Patch 249.00 OSF510X11-014	<p><b>Patch:</b> Vendor string displayed when running on COSIX64</p> <p><b>State:</b> Supersedes patches OSF510X11-010 (246.00), OSF510X11-013 (247.00)</p> <p>This patch fixes the following problems:</p> <ul style="list-style-type: none"><li>• 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).</li><li>• Fixes a problem where the X server does not display windows properly for the 128th and subsequent clients.</li><li>• Changes the X server to dynamically retrieve its vendor string information when running on COSIX64.</li></ul>
Patch 252.00 OSF510-173	<p><b>Patch:</b> Thread hang on NFS mounted file systems</p> <p><b>State:</b> New. Supersedes patch OSF510-174 (250.00)</p> <p>This patch corrects the following problems:</p> <ul style="list-style-type: none"><li>• Corrects a problem where a race condition in NFS can result in a kernel memory fault.</li><li>• Fixes a problem where threads can hang while renaming files on NFS mounted file systems.</li></ul>
Patch 255.00 OSF510-090	<p><b>Patch:</b> tar -F ignores files named err</p> <p><b>State:</b> New. Supersedes patch OSF510-164 (253.00)</p> <p>This patch corrects the following problems:</p> <ul style="list-style-type: none"><li>• 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</li><li>• 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.</li></ul>

---

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

---

Patch 260.00 OSF510-074A	<p><b>Patch:</b> Fix for V5.1 dynamic loader</p> <p><b>State:</b> Supersedes patches OSF510-005 (64.00), OSF510-113 (256.00), OSF510-105 (257.00), OSF510-205A (258.00)</p> <p>This patch fixes the following problems with the V5.1 dynamic loader:</p> <ul style="list-style-type: none"><li>• Allows the loader to properly ignore unreferenced symbols when loading a shared library with a dlopen call.</li><li>• Allows the loader to properly ignore loading a library with the correct library name but an incorrect library version.</li><li>• Fixes an /sbin/loader problem dealing with absolute value symbols when their value was -1.</li><li>• 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.</li><li>• A problem that may cause the /usr/ucb/spike post-link optimization tool to crash.</li><li>• 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.</li><li>• 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.</li><li>• Fixes a problem with /usr/ucb/ldd. Previously the _RLD_ARGS environment variable was not recognized.</li></ul>
Patch 262.00 OSF510-074B	<p><b>Patch:</b> Fix for loader and ldd</p> <p><b>State:</b> New</p> <p>This patch fixes the following problems:</p> <ul style="list-style-type: none"><li>• 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.</li><li>• Fixes a problem with /usr/ucb/ldd. Previously the _RLD_ARGS environment variable was not recognized.</li></ul>
Patch 265.00 OSF510-205B	<p><b>Patch:</b> loader does not report error</p> <p><b>State:</b> Supersedes patches OSF510-028 (78.00), OSF510-147 (263.00)</p> <p>This patch fixes the following problems:</p> <ul style="list-style-type: none"><li>• Fixes a problem where applying spike to some binaries results in a 100% performance degradation.</li><li>• 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.</li><li>• Fixes a problem that may cause the /usr/ucb/spike post-link optimization tool to crash.</li><li>• 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.</li></ul>

---



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

---

Patch 268.00 OSF510-165	<b>Patch:</b> Security (SSRT0690U) <b>State:</b> Supersedes patches OSF510-044 (55.00), OSF510-115 (266.00) This patch fixes the following problems: <ul style="list-style-type: none"><li>• 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.</li><li>• Fixes a possible handling problem with multibyte character boundary conditions in ksh script processing.</li><li>• Fixes two ksh problems that occur in multi-byte Asian locales.</li></ul>
Patch 270.00 OSF510DX-017	<b>Patch:</b> Updates Netscape Communicator to Version 4.76 <b>State:</b> Supersedes patch OSF510DX-001 (44.00) This patch corrects the following problems: <ul style="list-style-type: none"><li>• Fixes a security vulnerability (called the Brown Orifice) in Netscape Communicator Version 4.72 by updating Netscape Communicator to Version 4.75.</li><li>• Updates Netscape Communicator to Version 4.76 to fix missing default MIME types in Netscape Communicator 4.75.</li></ul>
Patch 278.00 OSF510-166	<b>Patch:</b> Cascaded switches may hang system at failover time <b>State:</b> New This patch fixes a problem where cascaded switches can hang the system at failover time.
Patch 280.00 OSF510X11-011	<b>Patch:</b> Fixes a memory leak in the X server <b>State:</b> Supersedes patch OSF510X11-002 (70.00) This patch fixes the following problems: <ul style="list-style-type: none"><li>• 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.</li><li>• Fixes synchronization and drawing problems in the X server for the PowerStorm 4D10T (ELSA Gloria Synergy, SN-PBXGK-BB) graphics card.</li><li>• 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).</li></ul>
Patch 283.00 OSF510-104	<b>Patch:</b> Security (SSRT0682U) <b>State:</b> New. Supersedes patch OSF510-096 (281.00) This patch corrects the following: <ul style="list-style-type: none"><li>• 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.</li><li>• 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.</li></ul>
Patch 285.00 OSF510-118	<b>Patch:</b> Fixes C++ runtime errors <b>State:</b> New This patch fixes C++ runtime errors.

---

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

---

Patch 287.00	<b>Patch:</b> Corrects blocks of erroneous pixels
OSF510X11-012	<b>State:</b> Supersedes patch OSF510X11-003 (119.00)
	This patch corrects the following:
	<ul style="list-style-type: none"><li>• Provides the Xserver library with a new graphics card.</li><li>• Corrects blocks of erroneous pixels left behind when dragging CDE application manager icons on the desktop.</li></ul>

---

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

---

Patch 290.00 OSF510-103	<p><b>Patch:</b> Fixes problems in the Tru64 UNIX Assembler</p> <p><b>State:</b> New. Supersedes patch OSF510-132 (288.00)</p> <p>This patch corrects the following:</p> <ul style="list-style-type: none"><li>• 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.</li><li>• 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.</li><li>• 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.</li><li>• The -arch and -tune command line switches were essentially being ignored.</li><li>• 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.</li><li>• 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.</li><li>• Code generated for loads with offsets larger than 32K is incorrect.</li><li>• Incorrect addresses are generated when symbolic arithmetic is used, and when the address in question extends beyond the initial 64K boundary of a section.</li><li>• A procedure with no instructions causes the assembler to segfault.</li><li>• A procedure with no instructions causes line number generation to segfault.</li><li>• Data declared using the .gpel32 directive was not being longword aligned.</li><li>• The relocation count for a program that contains a section that has in excess of 65535 relocations will be incorrect, resulting in a bad link and an invalid executable.</li><li>• 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.</li><li>• 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.</li><li>• 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.</li><li>• 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.</li></ul>
----------------------------	--

---

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

Patch 292.00 OSF510-148	<b>Patch:</b> Security (SSRT1-38) <b>State:</b> 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 294.00 OSF510-160A	<b>Patch:</b> Fixes a problem with the EVM daemon evmd <b>State:</b> 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	<b>Patch:</b> evmd crashes if rc.config contains a blank line <b>State:</b> New This patch fixes a problem with the EVM daemon, evmd, where it will crash if /etc/rc.config contains a blank line.
Patch 298.00 OSF510-210	<b>Patch:</b> Fix for kernel memory fault on EV6 systems <b>State:</b> New. Supersedes patch OSF510-004 (128.00) This patch corrects the following problems: <ul style="list-style-type: none"><li>• Fixes a cross RAD I/O hang problem with the ITPSA controller.</li><li>• Fixes a problem that can cause a simple lock timeout or a kernel memory fault on EV6 systems using the itpsa driver.</li></ul>
Patch 300.00 OSF510-080	<b>Patch:</b> Introduces the JJ printcap parameter <b>State:</b> New This fix 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.
Patch 302.00 OSF510DX-007	<b>Patch:</b> dop tool causes segmentation fault <b>State:</b> 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	<b>Patch:</b> Running cord on libraries causes infinite loop <b>State:</b> 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	<b>Patch:</b> Fixes a C++ compiler error <b>State:</b> New This patch fixes a C++ compiler error.
Patch 308.00 OSF510-106	<b>Patch:</b> Fixes C shell processing problems <b>State:</b> New This patch fixes C shell processing problems in the new zh_CN.GB18030 locale.
Patch 310.00 OSF510CDE-006	<b>Patch:</b> Fixes a problem on multi-head systems <b>State:</b> New This patch fixes a problem on multi-head systems in which the unlock display only works if the default display is screen 0.
Patch 312.00 OSF510-076	<b>Patch:</b> Fixes a problem of the ATM setup script failing <b>State:</b> New This patch fixes a problem of the ATM setup script failing when configuring an elan if the lane subsystem is not loaded.

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

---

Patch 314.00 OSF510-138	<b>Patch:</b> Security (SSRT0708U) <b>State:</b> New This patch fixes the following /usr/sbin/inetd problems: <ul style="list-style-type: none"><li>• 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.</li><li>• inetd can terminate without notice and without a core file.</li><li>• The disable keyword is being ignored when used in the /etc/inetd.conf.local configuration file.</li><li>• The -h option does not restart any inetd children to handle requests because the parent still thinks one is running.</li></ul>
Patch 316.00 OSF510-171	<b>Patch:</b> Attaching debugger to program causes program hang <b>State:</b> New This patch corrects a problem where attaching to a program with a debugger will cause periodic timers to be lost and will make the program hang.
Patch 318.00 OSF510-081	<b>Patch:</b> Fix for newgrp command <b>State:</b> 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	<b>Patch:</b> Fixes a problem in diskconfig <b>State:</b> 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 322.00 OSF510-142A	<b>Patch:</b> Fix for problems in Compaq C compiler <b>State:</b> Supersedes patch OSF510-016 (66.00) This patch fixes the following problems in the Compaq C compiler: <ul style="list-style-type: none"><li>• An optimizer problem that caused the wrong answer to be produced for a program involving tail recursion.</li><li>• An optimizer problem that caused a runtime error when compiling gcc using -feedback.</li><li>• An optimizer crash when compiling a program using -ieee and -tune ev6.</li><li>• An optimizer problem that caused a failure in the llogin UNIX command.</li><li>• An optimizer problem that caused incorrect run-time results for an OpenMP program.</li><li>• A problem in the parallel processing support library that caused incorrect run-time results for an OpenMP program.</li></ul>

---

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

---

Patch 324.00 OSF510-142B	<b>Patch:</b> Fix for libots3 <b>State:</b> New This patch fixes the following problem in the Compaq C compiler: <ul style="list-style-type: none"><li>• An optimizer problem that caused a failure in the llogin UNIX command.</li><li>• An optimizer problem that caused incorrect run-time results for an OpenMP program.</li><li>• A problem in the parallel processing support library that caused incorrect run-time results for an OpenMP program.</li></ul>
Patch 326.00 OSF510-082	<b>Patch:</b> Security (SSRT0672U) <b>State:</b> 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 328.00 OSF510-144	<b>Patch:</b> Fixes automount handling of nogrpid option <b>State:</b> New This patch fixes the automount handling of the nogrpid option.
Patch 330.00 OSF510-135	<b>Patch:</b> Write errors occur on soft mounted NFS file systems <b>State:</b> Supersedes patch OSF510-070 (132.00) This patch fixes the following problems: <ul style="list-style-type: none"><li>• Fixes an NFS file locking race.</li><li>• Corrects the problem with write errors seen on soft mounted NFS file systems. The error received is:  NFS3 RFS3_WRITE failed for server ncinfo: RPC: Server can't decode arguments</li></ul>
Patch 333.00 OSF510-112	<b>Patch:</b> Upgrades sys_check to v120 <b>State:</b> New. Supersedes patch OSF510-185 (331.00) This patch corrects the following problems: <ul style="list-style-type: none"><li>• Fixes errors generated by syscheck when NFS is not configured.</li><li>• Upgrades sys_check to V120.</li></ul>
Patch 335.00 OSF510-141	<b>Patch:</b> Fix for DVD file system problem <b>State:</b> New This patch addresses two issues with the DVD File system: <ul style="list-style-type: none"><li>• 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.</li><li>• Logical block numbers are not properly calculated after the first directory data read.</li></ul>
Patch 337.00 OSF510DX-008	<b>Patch:</b> Fix for bindconfig <b>State:</b> 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	<b>Patch:</b> Fix for dtpad <b>State:</b> 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	<b>Patch:</b> Fix for ksh hang <b>State:</b> 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	<b>Patch:</b> Fix for vi core dump <b>State:</b> 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	<b>Patch:</b> Cannot create builds with CAMDEBUG enabled <b>State:</b> New This patch fixes a problem of not being able to create builds with CAMDEBUG enabled.
Patch 347.00 OSF510-079	<b>Patch:</b> Fixes a problem of ATM signalling <b>State:</b> New This patch fixes a problem of ATM signalling going into connection released after a system reboot.
Patch 349.00 OSF510-121	<b>Patch:</b> Corrects memory leak in XTI socket code <b>State:</b> New This patch corrects a memory leak in the XTI socket code.
Patch 351.00 OSF510-093	<b>Patch:</b> Fix for TurboLaser panic <b>State:</b> 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	<b>Patch:</b> Fix for fsx utility <b>State:</b> New This patch fixes a problem in which the fsx utility would not correctly handle the -s switch.

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

---

Patch 358.00 OSF510-102	<b>Patch:</b> Fix for link errors <b>State:</b> Supersedes patches OSF510-022 (72.00), OSF510-153 (354.00), OSF510-108 (355.00), OSF510-120 (356.00) This patch corrects the following: <ul style="list-style-type: none"><li>• 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.</li><li>• Fixes a problem where the linker defined symbol <code>_fpdata</code> would end up being undefined if it was referenced by a program but not used by the linker.</li><li>• Fixes link errors encountered when linking with <code>-A</code>.</li><li>• Fixes two problems in the linker where it would erroneously report "multiply defined symbol" errors or "unresolved symbol" errors.<ul style="list-style-type: none"><li>– 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.</li><li>– Modifies the linker to cause it to rescan shared libraries before reporting unresolved symbols.</li></ul></li><li>• Fixes two errors that occur when using the <code>-f</code> switch with the linker (<code>ld</code>):<ul style="list-style-type: none"><li>– Using the <code>-f</code> switch produces link errors.</li><li>– Any unsupported switch beginning with <code>-f</code> gets interpreted to mean <code>-f</code>.</li></ul></li></ul>
Patch 360.00 OSF510DX-012A	<b>Patch:</b> Nodes in cluster unable to set high temp threshold <b>State:</b> 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	<b>Patch:</b> Cluster nodes unable to set high temp threshold <b>State:</b> 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	<b>Patch:</b> Security (SSRT1-15, SSRT0713U) <b>State:</b> 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 366.00 OSF510-125	<b>Patch:</b> Fixes ee driver for DE60x Ethernet cards <b>State:</b> New This patch addresses two problems with the ee driver for DE60x Ethernet cards. These problems affect all Tru64 UNIX systems containing ee cards: <ul style="list-style-type: none"><li>• Fixes a race condition where the card could stop receiving packets from the network under rare circumstances.</li><li>• Fixes the <code>lan_config</code> user options <code>-x</code> and <code>-s</code>.</li></ul>
Patch 368.00 OSF510-086	<b>Patch:</b> <code>rdist</code> utility causes segmentation fault <b>State:</b> New This patch corrects a problem in the <code>rdist</code> utility which was causing segmentation faults on files with more than one link.

---



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

---

Patch 370.00 OSF510-170	<b>Patch:</b> Fix for prpasswd daemon hang <b>State:</b> Supersedes patches OSF510-054 (145.00), OSF510-055 (146.00), OSF510-072 (148.00) This patch corrects the following: <ul style="list-style-type: none"><li>• 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.</li><li>• 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.</li><li>• Fixes a problem for Enhanced Security configurations where the Maximum Login Interval (u_max_login_intvl) field was being ignored for account templates.</li><li>• Fixes problems with the prpasswd daemon hanging when there are numerous background processes simultaneously attempting to authenticate users to the system in an Enhanced Security environment.</li></ul>
Patch 372.00 OSF510-127	<b>Patch:</b> Kernel memory fault occurs when using tablet <b>State:</b> New This patch fixes a kernel memory fault which occurs while using a tablet instead of a mouse.
Patch 374.00 OSF510-139	<b>Patch:</b> Hang seen on multi-CPU systems using NFS-over-TCP <b>State:</b> 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 376.00 OSF510-172	<b>Patch:</b> Fixes DS10/DS20 performance problems <b>State:</b> New This patch fixes DS10/DS20 performance problems introduced with the i2c driver by using thread blocking, rather than event_timeout() and DELAY().
Patch 378.00 OSF510-077	<b>Patch:</b> Fix for unaligned kernel space panic <b>State:</b> New This patch fixes a problem in which the system may panic with the panic string "Unaligned kernel space access from kernel mode".
Patch 381.00 OSF510-131	<b>Patch:</b> Security (SSRT0664U) <b>State:</b> New. Supersedes patch OSF510-100 (379.00) This patch corrects the following: <ul style="list-style-type: none"><li>• This patch corrects a problem with the ftpd daemon which could result in PC ftp clients hanging when transferring some files in ASCII mode.</li><li>• 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.</li></ul>
Patch 387.00 OSF510-143	<b>Patch:</b> CDFS media burned in 2001 shows the wrong dates <b>State:</b> New CDFS media burned in 2001 shows the wrong dates.

---

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

---

Patch 385.00 OSF510-075	<b>Patch:</b> Fixes problem in exit status value of swapon utility <b>State:</b> New This patch fixes a bug in the exit status value of the swapon utility.
Patch 389.00 OSF510-152	<b>Patch:</b> Corrects a problem with joind <b>State:</b> New This patch corrects a problem with joind which caused it to respond to certain client dhcp requests via the wrong port.
Patch 391.00 OSF510-128	<b>Patch:</b> System crash when accessing the FDI floppy <b>State:</b> Supersedes patch OSF510-058 (84.00) This patch corrects the following: <ul style="list-style-type: none"><li>• 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.</li><li>• Corrects a potential system crash when accessing the FDI floppy.</li></ul>
Patch 393.00 OSF510CDE-007	<b>Patch:</b> Fix for CDE window manager loop or abort problems <b>State:</b> Supersedes patch OSF510CDE-004 (160.00) This patch corrects the following: <ul style="list-style-type: none"><li>• Fixes a problem where the Window Manager (dtwm) intermittently hangs on a system which uses multiple displays.</li><li>• 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.</li></ul>
Patch 395.00 OSF510-189	<b>Patch:</b> Security (SSRT0713U) <b>State:</b> 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 399.00	<b>Patch:</b> Security (SSRT0700U)
OSF510-224	<b>State:</b> Supersedes patches 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), OSF510-163 (203.00), OSF510-155 (204.00), OSF510-194 (205.00), OSF510-122 (206.00), OSF510-157 (207.00), OSF510-134 (208.00), OSF510-129 (209.00), OSF510-181 (210.00), OSF510-109A (211.00), OSF510-180 (212.00), OSF510-092 (213.00), OSF510-167 (214.00), OSF510-158A (215.00), OSF510-179 (216.00), OSF510-178 (217.00), OSF510-068 (218.00), OSF510-199 (219.00), OSF510-156 (220.00), OSF510-169 (221.00), OSF510-162 (222.00), OSF510-200 (224.00)
	This patch corrects the following:
	<ul style="list-style-type: none"><li>• This patch is required in order to use the SuperDLT1 tape drive.</li><li>• 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.</li><li>• Prevents panics from occurring if AdvFS detects corruption in the per-fileset frags file and attempts to work around the corruption.</li><li>• Fixes AdvFS memory mapped file support so that it honors the noatimes and readonly mount options when updating file timestamps.</li><li>• 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.</li><li>• Provides an improvement to AdvFS performance when the first bytes of user data (and subsequent storage requests) is written to a domain.</li><li>• 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.</li><li>• 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.</li><li>• Fixes a kernel memory fault which can occur during scheduler load balancing on a NUMA system.</li></ul>

---

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

---

Patch 399.00 continued	<ul style="list-style-type: none"><li>• Fixes a panic that occurs in <code>madvise()</code> when called with <code>MADV_DONTNEED</code> when running in lockmode 4.</li><li>• Improves performance of HPTC programs on GS-series NUMA machines.</li><li>• Fixes a kernel memory fault which can happen when all the physical memory is in use.</li><li>• 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.</li><li>• Corrects a failure that is seen as a <code>user_cmd</code> timeout.</li><li>• Fixes a kernel memory fault when accessing a shared text segment after or during load balancing on a NUMA system.</li><li>• Fixes a bug that, when <code>fuser -k</code> is issued on a dismounted NFS mount point in which a process is running, a hang will occur.</li><li>• 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.</li><li>• Improves webserver performance, fixes an IPV6 related crash, and a hang in <code>soclose()</code>.</li><li>• Fixes problems for threaded applications running on Tru64 UNIX V5.1</li><li>• <code>sbin/dd</code> has been made non-threaded. This is to avoid problems while installing patches that are incompatible with the running kernel. <code>/usr/bin/dd</code> is not affected by this patch.</li><li>• Fixes SPECweb99 <code>httpd</code> hangs in <code>umc_get_page()</code> routine waiting for the page.</li><li>• Includes performance fixes for systems doing raw I/O, raw async I/O, and systems with large disk farms (high disk count).</li><li>• Enables the <code>getconf</code> command to return the abbreviated vendor name correctly.</li><li>• Provides the device driver for a new graphics card.</li><li>• Fixes a problem where some network-based multimedia applications will cause a kernel memory fault when exiting.</li><li>• Provides support for the DEGPA-TA (1000BaseT) Gigabit Ethernet device.</li><li>• Fixes a potential deadlock on systems using shared memory segments and granularity hints. This can occur when allocating a <code>gh</code> region larger than the available free memory.</li><li>• Improves UDP performance by removing an unneeded lock from the UDP output path.</li><li>• Fixes a panic in <code>in_pcbfree()</code> when NFS is implemented over TCP.</li><li>• 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.</li><li>• 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.</li><li>• 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 <code>vdIoLock</code> because of a large number of buffers on the <code>SmoothSync</code> queues.</li></ul>
---------------------------	--

---

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

---

Patch 399.00 continued	<ul style="list-style-type: none"><li>• 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.</li><li>• Fixes inaccuracy problems when using setrlimit/getrlimit with a threaded application.</li><li>• Addresses multiple issues for the KZPCC family of RAID Array 2000 (RA2000) controllers:<ul style="list-style-type: none"><li>– Errors seen when concurrent opens are issued to separate logical partitions on the same logical device.</li><li>– Change to the preferred chunk size from 16 KB to 64 KB which may increase data transfer rates.</li></ul></li><li>• Fixes a hang seen while running collect and the vdump utility. This patch prevents the hang in tok_wait from occurring.</li><li>• Prevents stat(), lstat(), fstat(), statfs(), fstatfs(), getmntinfo(), and getfsstat() from returning EOVERFLOW errors for programs compiled on Tru64 UNIX V4.0 or earlier.</li><li>• Fixes a problem where threads can hang in x_load_inmem_xtnt_map().</li><li>• Fixes a kernel memory fault when writing to /proc, while anon_rss_enforce is set to 2.</li><li>• Fixes an issue with lightweight wiring of pages and shared memory regions.</li><li>• 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.</li><li>• 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.</li><li>• 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.<p>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.</p><p>The conditions under which this potential problem may occur are as follows:</p><ul style="list-style-type: none"><li>– 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).</li><li>– Some but not all of the pages are still resident in Unified Buffer Cache (UBC) memory.</li></ul><p>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.</p><p>Applications that use direct I/O, such as Oracle, could be affected.</p></li><li>• This patch addresses two types of system crashes:<ul style="list-style-type: none"><li>– Crash caused by VM hash corruption, kernel memory fault.</li><li>– Crash caused by a lock hierarchy violation.</li></ul></li></ul>
---------------------------	---

---

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

---

Patch 399.00 continued	<ul style="list-style-type: none"><li>• 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.</li><li>• 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.</li><li>• Fixes issues with memory allocation attributes.</li><li>• 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.</li><li>• Fixes several virtual memory algorithms related to the allocation and freeing of pages within the kernel.</li><li>• 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().</li><li>• 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.</li><li>• Corrects an AdvFS panic which can occur during a rmfset operation, causing the following panic string:  rbf_delete_int: can't find bf attributes</li><li>• Fixes an issue with some remote ioctls for tape/changer drivers not working in a cluster.</li><li>• Fixes a panic which comes from a page fault on a user buffer while already holding the write lock.</li><li>• 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.</li><li>• Fixes a problem in which the system panicked with a kernel memory fault while the class scheduler was being configured.</li><li>• 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.</li></ul>
---------------------------	---

---

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

---

Patch 399.00 continued	<ul style="list-style-type: none"><li>• Fixes the following system panics:<ul style="list-style-type: none"><li>– 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.</li><li>– A "panic: vm_page_activate: already active" panic that can occur on a system during memory shortages.</li><li>– 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.</li></ul></li><li>• Fixes a problem in which a heavy load placed on an HSG80 can disable the device.</li><li>• 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.</li><li>• Fixes a system crash that could occur when calling nmadvise.</li><li>• 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.</li><li>• Eliminates a kernel memory fault in AdvFS.</li><li>• 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</li><li>• 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().</li><li>• Fixes a lockmode 4 panic in netisr_del_rad where netisr_del_rad attempted to release a lock it did not hold.</li><li>• Corrects the use of Granularity Hints in a threaded application program.</li><li>• Fixes a problem with writing out crashdumps on systems with their swap on Fibrechannel.</li></ul>
---------------------------	---

---

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

---

Patch 399.00 continued	<ul style="list-style-type: none"><li>• Fixes a kernel memory fault and invalid memory ifetch panic which can occur in AlphaServer SC systems running Quadrics' RMS software.</li><li>• 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.</li><li>• Corrects the behavior of the FIONBIO, FIOASYNC, and FIONREAD ioctls in a cluster environment. These commands would fail, returning ENOTTY when they should have succeeded.</li><li>• Fixes a problem in which the system call fcntl(fd, F_DUPFD, 15) fails with "too many files" even after fd limits have been increased.</li><li>• Corrects two problems with the scheduler:<ul style="list-style-type: none"><li>– Enables NUMA load balancing in other processor sets then the default processor set (pset 0).</li><li>– Enables the processor to do load balancing for multi-threaded applications.</li></ul></li><li>• Provides support for activating temporary data logging on a mount point.</li><li>• Fixes a hang in the UFS file system.</li><li>• Fixes kernel build failures due to an undefined ss_sched function.</li><li>• Fixes a problem with the execution of interpreter programs failing with a "file not found" error if the the total space used by the environment variables and command arguments is close to a multiple of 8K (page size).</li><li>• Provides full KZPCC support in Version 2.0 of the I2O block storage driver. Restriction: For TCR V5.1 installations, KZPCC support is restricted to data-only service; devices on the KZPCC controller cannot be used for system or boot partitions in a cluster. Additionally, this patch fixes the problem where extraneous console messages will appear when hardware is added or deleted.</li><li>• Fixes a performance problem with V5.1 where threads doing large I/O transfers could spend excess time in ubc_page_alloc().</li><li>• Fixes nmadvise with a modification to VM to allow migration of shared memory.</li><li>• Provides functions to support EMC storage boxes that support Persistent Reserves (SCSI command set) as defined by the final SCSI specification.</li><li>• Fixes a kernel memory fault in GS series systems which have mixed revision PCI adapters.</li><li>• Fixes the following two issues:<ul style="list-style-type: none"><li>– A "u_anon_free: page_busy" system panic when using System V shared memory locked by a single process.</li><li>– Failures ranging from uninitialized simple_lock panics, kernel memory fault panics, and process hangs, on GS320/160/80 systems configured with at least one memory less quad.</li></ul></li></ul>
Patch 401.00 OSF510-176A	<p><b>Patch:</b> Fixes POSIX message queue issues</p> <p><b>State:</b> New</p> <p>This patch fixes POSIX message queue issues seen with mq_open() and other calls with messaging.</p>

---



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

---

Patch 403.00 OSF510-176B	<b>Patch:</b> Fix for POSIX 4 message queue <b>State:</b> New This patch fixes POSIX message queue issues seen with mq_open() and other calls with messaging.
Patch 405.00 OSF510-176C	<b>Patch:</b> POSIX 4 message queues not following standard <b>State:</b> New This patch fixes POSIX message queue issues seen with mq_open() and other calls with messaging.

---

---

---



---

## Summary of TruCluster Software Patches

This chapter summarizes the TruCluster software patches included in Patch Kit-0003.

Table 3–1 lists patches that have been updated.

Table 3–2 provides a summary of patches in Patch Kit-0003.

**Table 3–1: Updated TruCluster Software Patches**

Patch IDs	Change Summary
Patches 4.00, 9.00, 17.00, 41.00	New
Patches 2.00, 13.00, 18.00, 19.00, 20.00, 21.00, 22.00, 23.00, 24.00	Superseded by Patch 26.00
Patch 11.00	Superseded by Patch 30.00
Patch 5.00, 7.00	Superseded by Patch 32.00
Patch 15.00, 33.00, 34.00, 35.00, 36.00, 37.00	Superseded by Patch 39.00

**Table 3–2: Summary of TruCluster Patches**

Patch IDs	Abstract
Patch 4.00 TCR510DX-001	<b>Patch:</b> Fix for Cluster Alias Manager system management tool <b>State:</b> New This patch fixes the Cluster Alias Manager system management tool from crashing and displaying errors.
Patch 9.00 TCR510-001	<b>Patch:</b> Initializing the MC-API results in system crash <b>State:</b> New 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.
Patch 17.00 TCR510-018	<b>Patch:</b> Removes rmerror_int diagnostic messages <b>State:</b> New This patch eliminates unnecessary rail failovers in vhub configurations and removes rmerror_int diagnostic messages.

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

---

Patch 26.00 TCR510-008	<p><b>Patch:</b> Security (SSRT0691U)</p> <p><b>State:</b> 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)</p> <p>This patch corrects the following:</p> <ul style="list-style-type: none"><li>• 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.</li><li>• Provides a small TPC-C performance optimization to <code>cfsspec_read</code> for reporting TPC-C single node cluster numbers.</li><li>• 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.</li><li>• During backup stage of <code>clu_upgrade</code> setup 1, <code>clu_upgrade</code> is unable to determine the name of the kernel configuration file.</li><li>• <code>clu_upgrade</code> does not check the availability of space in <code>/</code>, <code>/usr</code>, and <code>/usr/i18n</code>.</li><li>• During the preinstalled phase, <code>clu_upgrade</code> will ignore a no answer when the user is prompted, during an error condition, whether they wish to continue.</li><li>• <code>clu_upgrade</code> incorrectly assumes that if the directory <code>/usr/i18n</code> exists, then it is in its own file system.</li><li>• After the <code>clu_upgrade</code> clean phase, the final step of <code>clu_upgrade</code>, no message is displayed that leads the user to believe they have completed the upgrade. Only the prompt is returned and the <code>clu_upgrade -completed clean</code> command reports that the clean had not completed.</li><li>• <code>clu_upgrade</code> can display "Could not get property..." and "...does not exist" type of error messages during the undo install phase.</li><li>• The <code>clu_upgrade</code> undo switch command, after completing a <code>clu_upgrade</code> switch command, should display an error message instead of claiming it has succeeded.</li><li>• Fixes a problem with disaster recovery whereby the node being restored will hang on boot.</li><li>• 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.</li><li>• 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 <code>mknod(2)</code>.</li><li>• Corrects a problem in which a cluster member will panic with the patch string "lock_terminate: lock held" from <code>cinactive()</code>.</li></ul>
---------------------------	---

---

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

---

Patch 26.00 continued	<ul style="list-style-type: none"><li>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-&gt;tcb_flags &amp; TOK_GIVEBACK) == 0</li><li>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.</li><li>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.</li></ul>
Patch 30.00 TCR510-024	<p><b>Patch:</b> Corrects incorrect warning message <b>State:</b> Supersedes patch TCR510-007 (11.00) This patch corrects the following:</p> <ul style="list-style-type: none"><li>corrects a problem in which the RDG subsystem will stop sending messages even though there are messages which are deliverable.</li><li>Fixes an incorrect display of the following warning message at boot time:  rdg: failed to start context rcvq scan thread</li></ul>
Patch 32.00 TCR510-023	<p><b>Patch:</b> ring_rcv does not handle change in channel numbers <b>State:</b> Supersedes patches TCR510-002 (5.00), TCR510-003 (7.00) This patch corrects the following:</p> <ul style="list-style-type: none"><li>Fixes an occasional cluster hang which can occur after a Memory Channel error.</li><li>Fixes a kernel memory fault which occurs in the ics_mct_ring_rcv() 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.</li><li>Fixes a problem in ICS where ring_rcv() does not properly handle a change in channel numbers. The fix will, in turn, improve validation of the connection structure on node joins.</li></ul>

---

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

---

Patch 39.00 TCR510-012	<p><b>Patch:</b> System panics while doing tape failovers</p> <p><b>State:</b> 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)</p> <p>This patch corrects the following:</p> <ul style="list-style-type: none"><li>• Fixes two TruCluster problems:<ul style="list-style-type: none"><li>– If a Quorum disk is manually added by the command <code>clu_quorum -d add</code>, the disk becomes inaccessible because the PR flag is not being cleaned up. The same command will work in the next reboot.</li><li>– A cluster member cannot boot under a specific hardware setup. The CFS mount fails because of the PR flag is not cleaned up.</li></ul></li><li>• 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.</li><li>• Fixes an issue with a tape/changer failing to correctly report a close failure of a device in a cluster environment.</li><li>• Fixes a problem which results in a system panic while doing tape failovers.</li><li>• Fixes a node panic during fiber port disables.</li><li>• Fixes an issue with a tape/changer giving back “busy on open” if a close from a remote node failed.</li><li>• 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.</li><li>• Fixes an issue with requests being stuck on a failed disk in a cluster.</li></ul>
Patch 41.00 TCR510-019	<p><b>Patch:</b> Cluster members not able to route an alias</p> <p><b>State:</b> New</p> <p>This patch corrects the following:</p> <ul style="list-style-type: none"><li>• Fixes the <code>cluamgr</code> command where it will display the alias status even if no cluster member has joined the alias.</li><li>• Fixes a problem in which <code>rpc</code> requests to the cluster alias may fail with "RPC timeout" message.</li></ul>

---

---

---