

# Tru64 UNIX 5.1 and TruCluster 5.1

---

## Patch Summary and Release Notes for Patch Kit-0001

**October 2000**

This manual describes the release notes and contents of Patch Kit-0001. 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*.

---

© 2000 Compaq Computer Corporation

COMPAQ and the Compaq logo are registered in the U.S. Patent and Trademark Office. Alpha, AlphaServer, NonStop, TruCluster, Tru64, and VMS are trademarks of Compaq Computer Corporation.

Microsoft and Windows NT are registered trademarks of Microsoft Corporation. Intel, Pentium, and Intel Inside are registered trademarks of Intel Corporation. UNIX is a registered trademark and The Open Group is a trademark of The Open Group in the United States and other countries. Other product names mentioned herein may be the trademarks of their respective companies.

Possession, use, or copying of the software described in this publication is authorized only pursuant to a valid written license from Compaq Computer Corporation or an authorized sublicensor.

Compaq Computer Corporation shall not be liable for technical or editorial errors or omissions contained herein. The information in this document is subject to change without notice.

---

# Contents

## About This Manual

### 1 Release Notes

1.1	Required Storage Space .....	1-1
1.2	New dupatch Features .....	1-2
1.2.1	Patch Installation from Multiuser Mode .....	1-2
1.2.2	Automatic Kernel Build .....	1-2
1.2.3	Patch Installation from a Pseudo-Terminal .....	1-3
1.3	Release Note for Tru64 UNIX 5.1 Patch 84.00 .....	1-3
1.4	Release Note for Tru64 UNIX Patch 44.00 .....	1-3
1.5	Release Note for TruCluster Server .....	1-4

### 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 .....	2-2
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-0001 for the Tru64™ UNIX 5.1 operating system and TruCluster™ 5.1 software 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 *Installation Guide*
- Tru64 UNIX *System Administration*
- TruCluster Server *Software Installation*
- TruCluster Server *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](mailto: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-0001.

### 1.1 Required Storage Space

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

#### Base Operating System

- Temporary Storage Space

A total of ~250 MB of storage space is required to untar this patch kit. 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 ~31.5 MB of storage space in `/var/adm/patch/backup` may be required for archived original files if you choose to install and revert all patches. See the *Patch Kit Installation Instructions* for more information.

Up to ~31.6 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 ~90 KB of storage space is required in `/var/adm/patch/doc` for patch abstract and README documentation.

A total of ~136 KB of storage space is needed in `/usr/sbin/dupatch` for the patch management utility.

#### TruCluster Server

---

##### Note

---

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.

---

- **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 ~33.8 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 ~33.9 MB of storage space in `/var/adm/patch` may be required for original files if you choose to install and revert all patches. See the *Patch Kit Installation Instructions* for more information.  
Up to ~98 KB of storage space is required in `/var/adm/patch/doc` for patch abstract and README documentation.  
A total of ~136 KB of storage space is needed in `/usr/sbin/dupatch` for the patch management utility.

## 1.2 New dupatch Features

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

### 1.2.1 Patch Installation from Multiuser Mode

You can now install patches when a system is in multiuser mode.

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

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

### 1.2.2 Automatic Kernel Build

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

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

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

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

### 1.2.3 Patch Installation from a Pseudo-Terminal

You can now install patches on the system from a pseudo-terminal (pty) while in single-user mode. To do this, log in to the system as root from a remote location and specify that the patches are to be installed in single-user mode. After all the patch prerequisites are completed, the system goes into single-user mode while it maintains the network connection for the root user. The system then installs the patches.

## 1.3 Release Note for Tru64 UNIX 5.1 Patch 84.00

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>

## 1.4 Release Note for Tru64 UNIX Patch 44.00

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. (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 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>

---

## 1.5 Release Note for TruCluster Server

During a rolling upgrade from TruCluster Server Version 5.1 to TruCluster 5.1 Patch Kit-0001, you may see the following messages. You can safely ignore these messages. The stage will complete successfully.

- During the switch stage of a rolling upgrade:

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

- During the clean stage of a rolling upgrade:

```
Deleting tagged files.
.....
.rmdir: /var/.clu_upgrade: File exists
```

---

## Summary of Base Operating System Patches

This chapter summarizes the base operating system patches included in Patch Kit-0001.

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 5.00, 7.00, 9.00, 11.00, 13.00, 15.00, 17.00, 19.00, 21.00, 34.00, 36.00, 38.00, 40.00, 42.00, 44.00, 47.00, 49.00, 51.00, 53.00, 55.00, 57.00, 59.00, 62.00,, 64.00, 66.00, 68.00, 70.00, 72.00, 74.00, 76.00, 78.00, 80.00, 82.00, 84.00, 86.00	New
Patches 1.00, 2.00, 3.00	Superseded by Patch 5.00
Patch 45.00	Superseded by Patch 47.00
Patch 60.00	Superseded by Patch 62.00
Patch 22.00, 23.00, 24.00, 25.00, 26.00, 27.00, 28.00, 29.00, 30.00, 32.00	Superseded by Patch 86.00

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

Patch IDs	Abstract
Patch 5.00 OSF510-037A	<p><b>Patch:</b> Fixes a hang problem in threaded programs</p> <p><b>State:</b> New. Supersedes patches OSF510-033 (1.00), OSF510-019 (2.00), OSF510-027 (3.00)</p> <p>This patch corrects the following problems:</p> <ul style="list-style-type: none"><li>• Fixes a problem of the <code>getaddrinfo()</code> 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 <code>atof()</code> and <code>strtod()</code> 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 <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>.</li></ul>
Patch 7.00 OSF510-037B	<p><b>Patch:</b> OSF510-037B</p> <p><b>State:</b> New</p> <p>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>.</p>
Patch 9.00 OSF510-046	<p><b>Patch:</b> Fix for subset installation problem</p> <p><b>State:</b> New</p> <p>This patch ensures that re-installing a software subset will not erase existing subset info, even if the re-install fails.</p>
Patch 11.00 OSF510-011	<p><b>Patch:</b> Fixes problem on GS80, GS160, GS320 systems</p> <p><b>State:</b> New</p> <p>This patch fixes a problem on AlphaServer GS80, GS160, and GS320 systems where, under specific set of unlikely circumstances, it is possible for revision 4 PCA hardware to falsely report PCI bus hang 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.</p>
Patch 13.00 OSF510-013	<p><b>Patch:</b> Fix for vrestore problems</p> <p><b>State:</b> New</p> <p>This patch fixes the following vrestore 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 hardlinks 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 <code>-l</code> option</li><li>• Corrupted property list information could cause an infinite loop.</li></ul>

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

---

Patch 15.00 OSF510-009A	<b>Patch:</b> libst shared library fix <b>State:</b> New This patch fixes a problem with two routines in the libst library, st_obj_open() and st_obj_write(). The ability to change a file permission using these two libst routines is denied if a group has write permissions.
Patch 17.00 OSF510-009B	<b>Patch:</b> libst static library fix <b>State:</b> New This patch fixes a problem with two routines in the libst library, st_obj_open() and st_obj_write(). The ability to change a file permission using these two libst routines is denied if a group has write permissions.
Patch 19.00 OSF510-036	<b>Patch:</b> Fix for booting problem via network interface <b>State:</b> New 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> New This patch corrects a stack overflow panic encountered during the startup of the system management daemon(smsd) on configurations with more than 255 devices.
Patch 34.00 OSF510-039B	<b>Patch:</b> Fix for kernel memory fault <b>State:</b> New This patch fixes problems for threaded applications running on Tru64 UNIX V5.1.
Patch 36.00 OSF510DX-002	<b>Patch:</b> Fix for dxaccounts problem <b>State:</b> New This patch fixes the following dxaccounts problems: <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>• dxaccounts dialog messages are incorrectly displayed when a user is added with no password entry.</li><li>• dxaccounts 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 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>• -x account_inactive   account_expiration flags do not set the attributes.</li></ul>

---

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

Patch 38.00 OSF510-021	<b>Patch:</b> Fix for panic that occurs when kloadsv is restarted <b>State:</b> New This patch fixes a system panic that may occur when /sbin/kloadsv is restarted.
Patch 40.00 OSF510X11-001	<b>Patch:</b> Fix for lbxproxy utility <b>State:</b> New This patch fixes a problem where the X windows lbxproxy utility, which is used to make Low Bandwidth X (LBX) connections to an X server, did not accept local connections.
Patch 42.00 OSF510-031	<b>Patch:</b> Fix for grep command <b>State:</b> New This patch fixes a problem with the grep command in which the options -p -v together do not produce any output.
Patch 44.00 OSF510DX-001	<b>Patch:</b> Fix for Netscape Communicator Version 4.72 <b>State:</b> New This patch fixes a security vulnerability (called the Brown Orifice) in Netscape Communicator Version 4.72 by updating Netscape Communicator to Version 4.75.
Patch 47.00 OSF510-029	<b>Patch:</b> Fixes a kernel panic caused by btcreate <b>State:</b> New. Supersedes patch OSF510-045 (45.00) 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></ul>
Patch 49.00 OSF510-024	<b>Patch:</b> Fixes the processing of export lists <b>State:</b> New This patch fixes the processing of export lists with / (slash) in them.
Patch 51.00 OSF510-043	<b>Patch:</b> Change to kloadsv and hotswapd entries <b>State:</b> New This patch changes the kloadsv and hotswapd entries in the /etc/inittab file. The change will prevent possible problems with dynamically loaded kernel modules when shutting down to single user mode.
Patch 53.00 OSF510-048	<b>Patch:</b> Fixes problem encountered on heavily loaded HSG80 <b>State:</b> New This fixes a problem encountered on a heavily loaded HSG80, where a device may become unavailable to other cluster members if a cluster node crashes at the same time an error occurs on that device.
Patch 55.00 OSF510-044	<b>Patch:</b> Security (SSRT0690U) <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 57.00 OSF510-041	<b>Patch:</b> Fix for panic or system hang that may occur on DS20E <b>State:</b> New 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.

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

---

Patch 59.00 OSF510-025	<b>Patch:</b> Fix for tagged-file induced auto mount requests <b>State:</b> New This patch avoids tagged-file induced automount requests in AutoFS.
Patch 62.00 OSF510-014	<b>Patch:</b> Panic occurs if AdvFS detects corruption <b>State:</b> Supersedes patch OSF510-010 (60.00) This patch corrects the following: <ul style="list-style-type: none"><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></ul>
Patch 64.00 OSF510-005	<b>Patch:</b> Fix for V5.1 dynamic loader <b>State:</b> This patch fixes the following two problems with the V5.1 dynamic loader: <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></ul>
Patch 66.00 OSF510-016	<b>Patch:</b> Fix for problems in Compaq C compiler <b>State:</b> New 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></ul>
Patch 68.00 OSF510-003	<b>Patch:</b> Fix for dump command <b>State:</b> New The patch fixes a problem where a user could not dump to a regular file.
Patch 70.00 OSF510X11-002	<b>Patch:</b> Fixes synchronization and drawing problems <b>State:</b> New 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></ul>
Patch 72.00 OSF510-022	<b>Patch:</b> Fixes a spike problem <b>State:</b> New This patch 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.

---

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

---

Patch 74.00 OSF510-018	<b>Patch:</b> Fixes environmental warning in GS systems <b>State:</b> New This patch fixes a problem on the Alphaserwer 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> New 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 78.00 OSF510-028	<b>Patch:</b> Fix for spike command <b>State:</b> New This patch fixes a problem where applying spike to some binaries results in 100% performance degradation.
Patch 80.00 OSF510-034	<b>Patch:</b> System crash on machine functioning as IPv6 router <b>State:</b> New This patch 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.
Patch 82.00 OSF510CDE-001	<b>Patch:</b> List of application groups is not recreated <b>State:</b> New This patch fixes a problem where the Common Desktop Environment (CDE) Application Manager did not recreate the list of application groups at login. After customizing the application groups, users would see the old groups instead of the new groups.
Patch 84.00 OSF510-058	<b>Patch:</b> Fix for floppy disk problem <b>State:</b> New 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, 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.

---

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

---

Patch 86.00 OSF510-059	<p><b>Patch:</b> Security (SSRT0700U)</p> <p><b>State:</b> New. Supersedes patches 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)</p> <p>This patch corrects the following:</p> <ul style="list-style-type: none"><li>• Fixes a kernel memory fault which can occur during scheduler load balancing on a NUMA system.</li><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 occurs when <code>fuser -k</code> is issued on a dismounted NFS mount point in which some 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></ul>
---------------------------	--

---

---

---



## Summary of TruCluster Software Patches

This chapter summarizes the TruCluster software patches included in Patch Kit-0001.

Table 3–1 lists patches that have been updated.

Table 3–2 provides a summary of patches in Patch Kit-0001.

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

Patch IDs	Change Summary
Patch 2.00, 4.00, 7.00, 9.00	New
Patch 5.00	Superseded by Patch 7.00

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

Patch IDs	Abstract
Patch 2.00 TCR510-004	<p><b>Patch:</b> Security (SSRT0691U)  <b>State:</b> New</p> <p>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.</p>
Patch 4.00 TCR510DX-001	<p><b>Patch:</b> Fix for Cluster Alias Manager system management tool  <b>State:</b> New</p> <p>This patch fixes the Cluster Alias Manager system management tool from crashing and displaying errors.</p>
Patch 7.00 TCR510-003	<p><b>Patch:</b> Cluster hang occurs after Memory Channel error  <b>State:</b> New. Supersedes patch TCR510-002 (5.00)</p> <p>This patch fixes 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 <code>ics_mct_ring_rcv()</code> routine. The kernel memory fault would be seen when a node is booting into the cluster, and can occur on the booting node or on another node.</li> </ul>
Patch 9.00 TCR510-001	<p><b>Patch:</b> Initializing the MC-API results in system crash  <b>State:</b> New</p> <p>This patch fixes a problem where on the Alphaserwer GS160 systems, initializing the MC-API results in the system crashing with a "kernel memory fault" message.</p>