

Tru64 UNIX 5.0A and TruCluster 5.0A

Patch Summary and Release Notes for Patch Kit-0003

May 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

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	Release Note for Tru64 UNIX Patch 75.00	1-2
1.4	Release Note for Tru64 UNIX Patch 307.00	1-2
1.4.1	3DLabs Oxygen VXI Driver Support	1-2
1.4.2	DEGPA-TA Gigabit Ethernet Device	1-3
1.5	Release Note for Tru64 UNIX Patch 312.00	1-4
1.6	Release Note for Tru64 UNIX Patch 315.00	1-4
1.7	Release Note for Tru64 UNIX Patch 407.00	1-4
1.8	Release Note for Tru64 UNIX Patch 428.00	1-5
1.9	Release Note for Tru64 UNIX Patch 420.00	1-6
1.10	Release Note for TruCluster Server	1-7

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 5.0A operating system and TruCluster™ 5.0A Server 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*
- dupatch(8) Reference Page
- 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 5.0A and TruCluster 5.0A 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 ~42 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 ~43 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 ~646 KB of storage space is required in `/var/adm/patch/doc` for patch abstract and README documentation.
A total of ~168 KB of storage space is needed in `/usr/sbin/dupatch` for the patch management utility.

TruCluster Server

- 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 ~77 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 ~78 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 ~6890KB 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 Release Note for Tru64 UNIX Patch 75.00

SysMan Station does not dynamically update changes to a device name. If you use `dsfmgr(8)` to change the `base_name` of a device while `smsd(8)` is running, any SysMan Station clients that connect to the running `smsd(8)` will reflect the old `base_name` in their views.

To obtain a correct view, restart the SysMan Station daemon `smsd(8)` by performing the following steps. If you are on a cluster, perform these steps on all affected cluster members.

1. Close all open SysMan Station client sessions.
2. Enter the following command:

```
# /sbin/init.d/smsd restart
```

1.4 Release Note for Tru64 UNIX Patch 307.00

This section contains release notes for Tru64 UNIX Patch 307.00.

1.4.1 3DLabs Oxygen VXI Driver Support

This patch provides the driver support for the 3DLabs Oxygen VX1 PCI graphics card. In order to obtain full support for this graphics card, you must also select Patch 315.00, which is the X server portion of the patch.

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 Ethernet card as described previously, you will need to rebuild the kernel. To do this, follow the steps given previously.

Unpatched `genvmunix` will not recognize the 3DLabs Oxygen VX1 PCI graphics card and will include generic VGA graphics support in the resulting kernel.

1.4.2 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.

Unpatched `genvmunix` will not recognize the new Ethernet card and will include generic VGA graphics support in the resulting kernel.

1.5 Release Note for Tru64 UNIX Patch 312.00

This release note describes changes to the `rexecd` reference page.

OPTIONS

- s Causes `rexecd` to check for the `ptys` keyword in the `/etc/securettys` file and to deny execution of the request if it is from root and on a pseudoterminal.

DESCRIPTION

6. The `rexecd` server then validates the user as is done at login time and, if started with the `-s` option, verifies that the `/etc/securettys` file is not setup to deny the user. If the authentication was successful, `rexecd` changes to the user's home directory, and establishes the user and group protections for the user. If any of these steps fail, the connection is aborted with a diagnostic message returned.

1.6 Release Note for Tru64 UNIX Patch 315.00

This patch provides the X server support for the new 3Dlabs Oxygen VX1 PCI graphics card. In order to obtain full support for this graphics card, you must also select Patch 307.00, 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>

1.7 Release Note for Tru64 UNIX Patch 407.00

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 named `floppy_CSP_v51.tar.gz`, available from:

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

1.8 Release Note for Tru64 UNIX Patch 428.00

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 V5.0A Patch Kit-0003 and V5.1 Patch Kit-0003.

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
***
```

1.9 Release Note for Tru64 UNIX Patch 420.00

This patch delivers Version 1.0-032 of the `libots3` library. Version 2.0 of `libots3` library is delivered with the Compaq FORTRAN Compiler, Versions 5.3 ECO1 and 5.4, or the Developers Tool Kit (DTK) (OTABASE subset). If `libots3 V2.0` is already installed on your system, and you install this patch, you will receive the following informational message:

Problem installing:

```
- Tru64_UNIX_V5.0A / Software Development Environment Patches:
```

```
Patch 00420.00 - Fix for parallel processing support library
```

```
./usr/shlib/libots3.so: is installed by:
```

```
OTABASE212
```

and can not be replaced by this patch.

This patch will not be installed.

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

```
# what /usr/shlib/libots3.so
```

```
libots3.a V2.0-094 GEM 27 Feb 2001
```

1.10 Release Note for TruCluster Server

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

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 219.00, 221.00, 238.00, 242.00, 279.00, 293.00, 296.00, 312.00, 315.00, 317.00, 328.00, 330.00, 332.00, 334.00, 336.00, 338.00, 340.00, 342.00, 348.00, 352.00, 354.00, 359.00, 361.00, 363.00, 365.00, 367.00, 371.00, 375.00, 377.00, 379.00, 385.00, 387.00, 391.00, 393.00, 396.00, 403.00, 405.00, 411.00, 414.00, 420.00, 422.00, 426.00, 430.00	New
Patches 68.00, 98.00	Superseded by Patch 223.00
Patches 80.00, 126.00	Superseded by Patch 225.00
Patches 13.00, 24.00, 39.00, 40.00, 92.00, 52.00, 87.00, 104.00, 105.00, 106.00, 107.00, 108.00, 109.00, 110.00, 111.00, 112.00, 114.00, 226.00, 227.00, 228.00, 229.00, 230.00, 231.00, 232.00	Superseded by Patch 234.00
Patch 19.00	Superseded by Patch 236.00
Patches 239.00, 240.00	Superseded by Patch 242.00
Patches 21.00, 79.00, 287.00	Superseded by Patch 289.00
Patch 97.00	Superseded by Patch 291.00
Patch 294.00	Superseded by Patch 296.00
Patches 45.00, 46.00, 44.00, 82.00, 102.00, 159.00, 85.00, 103.00, 186.00, 83.00, 297.00, 298.00, 299.00	Superseded by Patch 301.00
Patches 59.00, 161.00, 215.00, 302.00, 303.00, 304.00, 305.00	Superseded by Patch 307.00
Patch 12.00	Superseded by Patch 309.00
Patch 310.00	Superseded by Patch 312.00
Patch 313.00	Superseded by Patch 315.00
Patch 22.00	Superseded by Patch 319.00
Patch 71.00	Superseded by Patch 321.00
Patch 26.00, 101.00, 155.00, 157.00	Superseded by Patch 326.00
Patches 30.00, 198.00	Superseded by Patch 418.00
Patch 31.00	Superseded by Patch 350.00
Patches 202.00, 355.00	Superseded by Patch 357.00
Patch 33.00	Superseded by Patch 371.00
Patches 38.00, 380.00, 381.00	Superseded by Patch 383.00
Patch 57.00	Superseded by Patch 389.00

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

Patch 394.00	Superseded by Patch 396.00
Patches 84.00, 217.00	Superseded by Patch 407.00
Patch 209.00	Superseded by Patch 409.00
Patch 412.00	Superseded by Patch 414.00
Patches 36.00, 28.00, 29.00, 43.00, 49.00, 55.00, 56.00, 58.00, 16.00, 17.00, 18.00, 93.00, 88.00, 94.00, 96.00, 135.00, 136.00, 137.00, 138.00, 139.00, 141.00, 48.00, 77.00, 190.00, 60.00, 89.00, 243.00, 244.00, 245.00, 246.00, 247.00, 248.00, 249.00, 250.00, 251.00, 252.00, 254.00, 255.00, 256.00, 257.00, 258.00, 259.00, 260.00, 261.00, 262.00, 263.00, 264.00, 265.00, 266.00, 267.00, 268.00, 269.00, 270.00, 271.00, 272.00, 273.00, 274.00, 275.00, 277.00, 286.00, 416.00	Superseded by Patch 428.00
Patches 322.00, 324.00	Superseded by Patch 430.00

Table 2–2: Summary of Base Operating System Patches

Patch IDs	Abstract
Patch 1.00 OSF505CDE-001	Patch: CDE does not re-create list of application groups State: Existing This patch fixes a problem where the Common Desktop Environment (CDE) Application Manager did not re-create the list of application groups at login. After customizing the application groups, users would see the old groups instead of the new groups.
Patch 2.00 OSF505DX-002	Patch: Compaq SNMP subagent core dumps State: Existing This patch fixes a problem that causes Compaq SNMP subagent (cpq_mibs) to coredump at boot-up time or when being reinvoked, which results in an invalid display of information on Insight Manager web pages.
Patch 3.00 OSF505DX-003	Patch: Fixes automount problem State: Existing This patch fixes a problem that occurs when restarting all NFS daemons with the automount argument set to empty.
Patch 8.00 OSF505X11-001	Patch: Provides missing compose definitions for ISO8859-15 State: Existing This patch provides missing compose definitions in ISO8859-15-based locales for scaron, Scaron, zcaron, and Zcaron characters.
Patch 10.00 OSF505X11-003A	Patch: Fixes a problem with the svn widget of libDXm.so State: Existing This patch fixes a problem in which the svn widget of libDXm.so creates identical backgrounds and foregrounds.
Patch 11.00 OSF505X11-004	Patch: Fix for lbxproxy utility State: Existing This patch fixes a problem where the X windows lbxproxy utility that is used to make Low Bandwidth X (LBX) connections to an X server did not accept local connections.
Patch 14.00 OSF505-005	Patch: Updates the Danish (da_DK.ISO8859-1) locale State: Existing This patch updates the Danish (da_DK.ISO8859-1) locale to use all lowercase month names.
Patch 15.00 OSF505-006	Patch: Fixes a problem that occurs in multibyte locales State: Existing This patch fixes a problem that sometimes occurs when sorting large data files in a multibyte locale such as Japanese.
Patch 23.00 OSF505-014	Patch: Fixes a kernel memory fault when using ATM State: Existing This patch fixes a kernel memory fault when using ATM.
Patch 25.00 OSF505-016	Patch: Fix for VMAC functionality when used with NetRAIN State: Supersedes patch OSF505-011 (20.00) This patch corrects the following: <ul style="list-style-type: none">• Fixes a kernel memory fault in VMAC code if_addnewaddr().• Adds a fix to VMAC functionality when used with NetRAIN.
Patch 27.00 OSF505-018	Patch: Changes quotactl prototype to meet POSIX standards State: Existing This patch changes the quotactl prototype in /usr/include/ufs/quota.h to meet POSIX standards.

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

Patch 32.00 OSF505-023	Patch: Kernel panics Classical IP over lfa ATM driver State: Existing This patch fixes a kernel panic seen when running Classical IP over the lfa ATM driver. This panic would only occur in lockmode 4. If not in lockmode 4, the symptom would be a CPU hang.
Patch 35.00 OSF505-026	Patch: Fixes a problem with the find command State: Existing This patch fixes a problem where the find command fails to show filenames that start with a period.
Patch 37.00 OSF505-028	Patch: Fixes a tftpd problem State: Existing This patch fixes a tftpd problem. When responding to a broadcast read request and it would add the -b option to control whether to respond to any broadcasts.
Patch 41.00 OSF505-032	Patch: Corrects problem with the fgrep command State: Existing This patch corrects a problem with the fgrep command. When fgrep is used with the -s flag, all output is suppressed.
Patch 42.00 OSF505-033	Patch: Fixes problem with the restore command State: Existing This patch fixes a problem in which the restore command can fail with the following error: Cannot malloc space for property list
Patch 47.00 OSF505-038	Patch: UFS disk quotas are not updating automatically State: Existing This patch fixes a problem where UFS disk quotas are not updating automatically.
Patch 51.00 OSF505-043	Patch: Provides the latest driver for PowerStorm 4D10T State: Existing This patch provides the latest driver for the PowerStorm 4D10T (ELSA Gloria Synergy, SN-PBXGK-BB) graphics card and the latest graphics driver for the PCI To Ethernet/Graphics Combo Adapter (3X-DEPVD-AA).
Patch 53.00 OSF505-045	Patch: Fixes errors seen when compiling with the -om switch State: Existing This patch fixes three errors that are occasionally seen when compiling with the -om switch: om: fast access range error om: value(0x1201704de) not in range of GP table core dumping in the routine reloc_abs()
Patch 61.00 OSF505-055	Patch: Hardware manager inaccurately reports CPU speed State: Existing This patch fixes a problem where the hardware manager inaccurately reports a CPU speed that was one MHz less than the correct speed.
Patch 62.00 OSF505-056	Patch: Cursor displays incorrectly when image plane is set to 1 State: Existing This patch fixes a problem where the cursor is displayed incorrectly when the image plane is set to 1 and the mask plane is set to 0.

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

Patch 64.00 OSF505-058	Patch: Fixes btcreate and btextract problems State: Existing This patch fixes the following btcreate and btextract problems: <ul style="list-style-type: none">• The DEFAULT restore fails if disklabel is different.• The btcreate command does not wait long enough between vdumps for the next tape to be loaded by some media changers.
Patch 65.00 OSF505-059	Patch: Fixes a hang in the shutdown process State: Existing This patch fixes a hang in the shutdown process (shutdown now) of a system when a device has flow control switched off.
Patch 66.00 OSF505-060	Patch: Fixes kdbx extensions mount and swap State: Existing This patch fixes problems with the kdbx extensions mount and swap. Information about the file system type is incorrect in the mount command. The device name is missing in the swap command.
Patch 67.00 OSF505-062A	Patch: Fixes a problem with routines in the libst library State: Supersedes patch OSF505-025A (34.00) This patch corrects the following problems: <ul style="list-style-type: none">• 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 group has write permissions.• Fixes a segmentation fault problem with the profiling tool prof. The problem is in library routines that access the line number information in the symbol table, and can affect other commands that look at the symbol table.
Patch 69.00 OSF505-064	Patch: Updates the lfa ATM device driver to V1.0.17 State: Existing This patch updates the lfa ATM device driver to V1.0.17 and adds some enhancements as well as a fix for a kernel memory fault seen when either shutting down or restarting the device driver.
Patch 70.00 OSF505X11-003B	Patch: Static library fix for libDXm State: Existing This patch fixes a problem in which the svn widget of libDXm.so creates identical backgrounds and foregrounds.
Patch 72.00 OSF505-025B	Patch: Cannot change file permission using libst routines State: Existing This patch fixes a problem with two routines in the libst library, st_obj_open() and st_obj_write(). The ability to change a file permission using these two libst routines is denied if group has write permissions.
Patch 73.00 OSF505-062B	Patch: prof profiling tool causes segmentation fault State: Existing This patch fixes a segmentation fault problem with the profiling tool prof. The problem is in library routines that access the line number information in the symbol table, and can affect other commands that look at the symbol table.
Patch 74.00 OSF505-030B	Patch: Security (SSRT0636U) State: Existing A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability.

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

Patch 75.00 OSF505DX-008	Patch: Fix for System Management Station daemon State: Existing This patch fixes the following problems with the System Management Station daemon: <ul style="list-style-type: none">• The System Management Station daemon (smsd(8)) will intermittently crash.• The SysMan Station client will intermittently fail to launch a tool.
Patch 76.00 OSF505X11-006A	Patch: Security (SSRT0656U) State: Existing A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability.
Patch 81.00 OSF505-072	Patch: Fix for dn_setup core dump State: Existing This patch fixes a problem where /sbin/dn_setup will core dump during the boot process. The following error is displayed: /sbin/dn_setup: 1572936 Memory fault - core dumped
Patch 86.00 OSF505-070	Patch: Fix for rm_state_change panic State: Supersedes patch OSF505-057 (63.00) This patch corrects the following: <ul style="list-style-type: none">• Fixes a problem in the memory channel driver which could result in panics with rm-inconsistent local spinlock structures being logged.• Fixes a system panic that involves state changes on MC2 virtual Hub configurations. The panic message on the console is: rm_state_change: panic (cpu 0): ERROR: DATA APPEARS CORRUPTED
Patch 90.00 OSF505-081	Patch: versw command can core dump during rolling upgrade State: New This patch fixes a problem where the versw command can core dump during a rolling upgrade.
Patch 95.00 OSF505-082A	Patch: Overlap checking in MKFDMN and NEWFS fails State: Existing This patch fixes a problem where overlap checking in MKFDMN and NEWFS would fail for third-party drivers used in a cluster.
Patch 99.00 OSF505-082B	Patch: MKFDMN NEWFS fails for third party drivers in cluster State: Existing Fixes a problem where overlap checking in MKFDMN and NEWFS would fail for third party drives used in a cluster.
Patch 100.00 OSF505X11-006B	Patch: Security (SSRT0656U) State: Existing A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability.
Patch 116.00 OSF505-137B	Patch: Fixes a problem in uucp State: New This patch fixes a problem in uucp where uucp fails on systems names that are greater than seven characters.

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

Patch 118.00 OSF505-089	Patch: Corrects a problem in the lat driver State: New This patch corrects a problem in the lat driver which caused improper processing of the ioctl TCSBRK as well as the generation of spurious <BREAK> characters when the libc routine tcdrain() was used.
Patch 120.00 OSF505-120	Patch: System panic occurs when auditing is enabled State: New This patch fixes the problem where a system may panic with a kernel memory fault when auditing is enabled.
Patch 122.00 OSF505-080	Patch: Fixes a timeout table overflow system panic State: New This patch fixes a timeout table overflow system panic, especially in a clustered environment. This occurs when a bus reset in the isp driver did not restore the System Priority Level (spl), leaving it at an elevated level.
Patch 124.00 OSF505X11-008	Patch: Adds support for Euro character to keymap files State: New This patch adds support for the Euro character to keymap files.
Patch 128.00 OSF505-139B	Patch: Fix for threads created by taso programs State: New This patch ensures that threads created by programs linked -taso run on stacks with addresses that fit in the 31-bit taso range. Prior to this patch threads created by taso programs were run on stacks with non-taso addresses, which could result in truncated address values, and segmentation faults or data corruption depending on whether the truncated address is valid.
Patch 130.00 OSF505-096	Patch: Incorrect warning messages about mounted file systems State: New This patch prevents "not currently mounted" warning messages from being displayed for file systems you did not request to amount.
Patch 132.00 OSF505X11-012	Patch: Fix for tclhelp failure State: New This patch fixes a problem in which tclhelp and any other tool using #!/usr/bin/wishx as the interpreter fail when additional versions of tcl are installed in /usr/local.
Patch 134.00 OSF505-130	Patch: Fixes problems with vdf State: New This patch fixes two separate problems with vdf: <ul style="list-style-type: none">• vdf does not run at non-root level.• vdf may give incorrect information.
Patch 150.00 OSF505X11-010A	Patch: Fixes a memory leak in Xt State: New This patch 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.
Patch 152.00 OSF505X11-010B	Patch: Memory leak when creating and destroying widgets State: New This patch 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.

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

Patch 154.00 OSF505-095	Patch: Improper handling of PCI options cards State: Supersedes patch OSF505-046 (54.00) This patch corrects the following: <ul style="list-style-type: none">• Provides PCI Resource Management support for the Atalla AXL200 cryptographic accelerator card. It also fixes a problem where genvmunix does not boot on a system with an Atalla AXL200 card installed.• Fixes the improper handling of PCI options cards that use 64-bit BARs (Base Address Registers).
Patch 163.00 OSF505-087	Patch: Fixes conflicting cuserid declarations State: New This patch fixes conflicting cuserid() declarations. It also fixes existing prototype/definition conflicts that cause C++ compiler errors when using this function.
Patch 165.00 OSF505CDE-003	Patch: dtlogin core dumps from XDMCP clients State: New This patch fixes a problem where the Common Desktop Environment (CDE) login daemon, dtlogin, core dumps occasionally when servicing requests from XDMCP clients such as X terminals or PCs running X servers.

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

Patch 167.00 OSF505DX-009	<p>Patch: Fixes incorrect date and time stamp on new directory</p> <p>State: Supersedes patches OSF505DX-004 (4.00), OSF505DX-005 (5.00), OSF505DX-006 (6.00), OSF505DX-007 (7.00)</p> <p>This patch corrects the following problems:</p> <ul style="list-style-type: none">• Fixes a situation in which a system running ASU experiences dxaccounts crash problem when a user is deleted from PC User view.• Fixes the following cli command problems:<ul style="list-style-type: none">– Incorrect results of usermod -G command.– Not setting c2 security attributes values when useradd/usermod commands with -x account_inactive account_expiration are executed.– When running useradd X and useradd Y on the same machine but from separate terminals, two different types of contention error messages are displayed.– The following command does not display an error message, which it should when executed from a NIS client: usermod (or useradd) -x local=0'groupmod (or groupadd) -x local=0• Fixes the following dxaccount problems:<ul style="list-style-type: none">– The ability to change root's login/uid through cli/dxaccounts utilities.– The -t flag in useradd and usermod commands' usage displays an error message instead of adding or modifying the local user.– dxaccounts dialog messages are incorrectly displayed when a user is added with no password entry.– Unable to create a new user from the PC Users view on a system with ASU installed.– The following problems can occur with the dxaccounts application on ASU systems:<ul style="list-style-type: none">□ dxaccounts crashes when the root icon is double clicked.□ The full name of a new PC account is not mapped to a UNIX user.□ Erasing a PC account's fields does not work: the values erased remain.□ The default values of Home Directory, Login Script, and User Profile Path for a PC user are invalid.• 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.
Patch 170.00 OSF505-117	<p>Patch: ATM LAN emulation fails with ATM Meteor 351 board</p> <p>State: New. Supersedes patch OSF505-097 (168.00)</p> <p>This patch corrects the following:</p> <ul style="list-style-type: none">• When running ATM Lan Emulation, using more than four ATM Netrain interfaces can result in recursive calls causing a kernel stack not valid halt.• Fixes a problem of ATM LAN emulation failing to come up when the using the ATM Meteor 351 board.
Patch 172.00 OSF505-136	<p>Patch: Fixes problems with the collect command</p> <p>State: New</p> <p>This patch fixes several problems with the collect command and adds sysloging when collect suspends, resumes, or receives a signal.</p>

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

Patch 174.00 OSF505X11-009A	Patch: Fix for memory leaks in Xlib State: New. Supersedes patch OSF505X11-002 (9.00) This patch corrects the following: <ul style="list-style-type: none">• Fixes a problem in which some 8-bit characters cannot be entered directly from the keyboard when the Caps Lock setting is on.• 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.
Patch 176.00 OSF505X11-009B	Patch: Memory leaks occur when creating widgets State: New This patch 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.
Patch 178.00 OSF505-110	Patch: Incorrect bcache size returned to kernel from HWRPB State: New This patch corrects the following. <ul style="list-style-type: none">• A problem that caused the device_tables.h file to be unusable with C++. This problem occurred on Professional Workstation 900 and 1000 systems and AlphaServer DS10, DS20, DS20E, and ES40 systems.• A problem that caused an incorrect bcache size to be returned to the kernel from the HWRPB. This problem occurred on Professional Workstation 900 and 1000 systems and AlphaServer DS10, DS20, DS20E, ES40, GS80, GS160, and GS320 systems
Patch 180.00 OSF505X11-011A	Patch: Fixes memory leak in libXm State: New This patch fixes various memory leaks in the Motif library (libXm) that could occur when creating and destroying Motif List, Text, and TextField widgets.
Patch 182.00 OSF505X11-011B	Patch: libXm memory leak when creating widgets State: New This patch fixes various memory leaks in the Motif library (libXm) that could occur when creating and destroying Motif List, Text, and TextField widgets.
Patch 184.00 OSF505-127	Patch: Bootlink can fail on AlphaStations 600, 600A, 500/400 State: New This patch fixes a problem in which the bootlink can fail on Alphastations 600, 600A, and 500/400.
Patch 188.00 OSF505-090	Patch: advscan does not display bootable partitions properly State: Existing When a disk partition exactly overlaps an AdvFS partition, the advscan utility would erroneously think both partitions belong in the domain. This patch fixes a problem where advscan -a -g does not display bootable partitions properly.
Patch 192.00 OSF505-121	Patch: Fix for what command State: New This patch fixes a problem in the what command. This command was unable to process more than one input file at once.
Patch 194.00 OSF505-146	Patch: Fixes potential source code computability problem State: New This patch fixes a potential source code computability problem with certain third party (non-Compaq) device drivers.

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

Patch 196.00 OSF505-107	Patch: Security (SSRT0683U) State: New A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability.
Patch 200.00 OSF505CDE-002	Patch: Fix for dtmail problem State: New This patch fixes a dtmail problem in which a From line with quotes in it incorrectly finds the date of the mail message. This error is displayed on the main screen under the header Date and Time and shows up as Dec. 31 or as a blank field.
Patch 205.00 OSF505-125	Patch: Corrects problem with mv command deleting files State: Supersedes patch OSF505-115 (203.00) This patch corrects the problem with the mv(1) command deleting files in the directory when the user moves a directory to itself.
Patch 207.00 OSF505-124	Patch: Potential hang on booting a cluster State: New This patch is to prevent a potential hang on booting a cluster when more than one node is being booted simultaneously.
Patch 211.00 OSF505-108	Patch: Fixes cron problems State: Supersedes patch OSF505-042 (50.00) This patch corrects the following: <ul style="list-style-type: none">• Fixes a problem where some crontab jobs would run multiple times in the same minute.• The cron daemon does intensive logging and fills up the disk.• Multiple cron daemons continue to run and consume system resources due to the fact that after a user is deleted from the system there are still jobs running on the users behalf.
Patch 213.00 OSF505DX-010	Patch: Fixes problem causing diskconfig to issue error message State: New This fixes a problem that was causing diskconfig to issue the following error message upon startup: can't read "tminor": no such variable
Patch 219.00 OSF505-184	Patch: Corrects voldctl stop command behaviour for clusters State: New This patch corrects the voldctl stop command behaviour for cluster support.
Patch 221.00 OSF505-165	Patch: fixso command causes segmentation fault State: New This patch fixes a problem with the /usr/ucb/fixso command that can cause a segmentation fault.

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

Patch 223.00 OSF505-221	<p>Patch: Fix for vdump and vrestore</p> <p>State: Supersedes patches OSF505-063 (68.00), OSF505-077B (98.00)</p> <p>This patch fixes the following vrestore problems:</p> <ul style="list-style-type: none">• A previous patch caused incomplete restores.• A warning message is displayed when the path for the first file in a group of hardlinks is created without using original protection codes and property lists.• A warning message is displayed and vrestore aborts if it fails to malloc space for a property list.• A message that had been inserted at the end of the message file had the wrong message category (this could cause messaging confusion).• An uninitialized variable in the code that restores property lists could cause malloc failures, memory faults, "error setting extended attributes", and infinite loops using the -l option• Corrupted property list information could cause an infinite loop. <p>This patch fixes the following pax and vdump problems:</p> <ul style="list-style-type: none">• The pax/tar command opens and truncates pre-existing files when extracting from an archive. This can cause problems when performing an update install.• The vdump command will backup automount symbolic links as files in a directory section. A restore of this link would then prevent automount from changing a directory file to a symbolic link file. <p>This patch fixes the following problems with the vdump command:</p> <ul style="list-style-type: none">• Failed to flag compressed extended attributes records that are split across a vdump BLOCK boundary.• Overrides the -D option when source path describes a root fileset Note: If you want to backup quota files, you must not use the -D option.• Corrects "Rewinding" message to avoid a segfault with Internationalized messages. <p>This patch fixes the following problems with the vrestore command:</p> <ul style="list-style-type: none">• Fails to properly handle extended attributes records in compressed archives. This results in malloc failures, proplist inconsistencies, program abort, program crashes due to segfault or invalid memory access, and the display of the error message "error setting extended attributes".• Fails to set extended attributes due to confusion over selective restore of the file or directory associated. Also results in the display of the error message "error setting extended attributes".• Selective restore of hardlinked files is incomplete when they exist in different directories (fails to create directory for second occurrence of file with same inode number).• The -Q option is added to vrestore to allow the user to request ignoring the quota files (thus avoiding the time it takes to process them).
----------------------------	---

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

Patch 225.00 OSF505-204	<p>Patch: Fix for threaded applications problem</p> <p>State: Supersedes patches OSF505-068 (80.00), OSF505-139A (126.00)</p> <p>This patch corrects the following:</p> <ul style="list-style-type: none">• Fixes a problem where threaded applications built on DIGITAL UNIX V3.2-era systems may encounter an unresolved reference to <code>_pthread_init_routine</code> when run on a Tru64 UNIX V5.0A system.• Ensures that threads created by programs linked <code>-taso</code> run on stacks with addresses that fit in the 31-bit <code>taso</code> range. Prior to this patch threads created by <code>taso</code> programs were run on stacks with non-<code>taso</code> addresses, which could result in truncated address values, and segmentation faults or data inconsistencies depending on whether the truncated address is valid.• This patch fixes four problems for threaded applications on Tru64 UNIX V5.0A:<ul style="list-style-type: none">– A memory leak when the <code>pthread_attr_setname_np</code> function is used.– <code>pthread_setname_np</code> occasionally returning an <code>EINVAL</code> error.– VM subsystem can cause deadlocks on <code>pthread</code> library internal mutexes.– Threaded processes looping in internal routine <code>__krnUnlock</code>.
----------------------------	---

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

Patch 234.00	Patch: Security (SSRT0636U)
OSF505-210	State: Supersedes patches OSF505-004 (13.00), OSF505-015 (24.00), OSF505-030A (39.00), OSF505-031 (40.00), OSF505-061 (92.00), OSF505-044 (52.00), OSF505-071 (87.00), OSF505-105 (104.00), OSF505-137A (105.00), OSF505-128 (106.00), OSF505-135 (107.00), OSF505-086 (108.00), OSF505-116 (109.00), OSF505-118 (110.00), OSF505-119 (111.00), OSF505-113 (112.00), OSF505-099 (114.00), OSF505-241 (226.00), OSF505-168 (227.00), OSF505-163 (228.00), OSF505-228 (229.00), OSF505-153 (230.00), OSF505-191 (231.00), OSF505-209 (232.00)
	This patch corrects the following:
	<ul style="list-style-type: none">• The regular expression logic used by <code>grep</code> did not identify matches that involved expressions with multiple subexpressions and alternate patterns.• Corrects the error handling when invalid multibyte sequences are encountered by the <code>vi</code>, <code>ex</code>, or <code>more</code> commands.• Fixes a problem in <code>libc</code> where <code>gmtime()</code> would return a <code>tm</code> struct containing an incorrect <code>tm_zone</code> abbreviation if previous calls to both <code>gmtime()</code> and <code>localtime()</code> were made.• A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability.• Fixes a problem in <code>libc</code> that affects debugger tracebacks of code containing split procedures.• Corrects a "permission denied" error when writing to the <code>/var/tcb/files/dblogs/[logfile]</code> while running <code>pop3d</code> and enhanced security.• Corrects a problem of the <code>rsh</code> command displaying a warning message instead of the <code>rsh</code> command output when C2 security is configured.• The <code>sia_get_groups()</code> interface where threads other than the main thread in a multi-threaded programs do not receive the correct values in the returned group list.• The <code>sia_get_groups()</code> interface where threads other than the main thread in a multi-threaded programs do not receive the correct values in the returned group list.
	<code>it.log: db_load: /tcb/files/auth.db2: Bad file number</code> <code>it.log: db_load: /var/tcb/files/auth.db2: Bad file number</code>
	<ul style="list-style-type: none">• Fixes a problem that causes <code>rshd</code> and other programs to core dump.h• Fixes a problem in <code>uucp</code>. <code>uucp</code> fails on systems names that are greater than seven characters.• Fixes a problem where a TZ environment variable setting of ":" yields incorrect (or missing) time zone information after calling <code>tzset()</code> and incorrect error reporting from <code>mktime()</code>.• Fixes a problem for those applications that assume initial allocations of memory from the C run-time library's <code>malloc()</code> function will return only zero-filled memory.• Adds a NULL to the resulting string output of <code>swprintf()</code> calls.

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

Patch 234.00 continued	<ul style="list-style-type: none">• Fixes a problem in libc that affects the mktemp, tmpnam, and tempnam functions. The temporary file names that were generated might contain the # character, which violates the file naming standard and may cause problems if a shell script containing a reference to that filename is generated.• 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 option and is allowed to change to a new password.• Fixes a problem in an Enhanced Security configuration. This patch restores the capability of being able to su to a user as root without being prompted or having to know the user's password.• Fixes a problem for Enhanced Security configurations where the Maximum Login Interval (u_max_login_intvl) field was being ignored for account templates.• Fixes a problem that occurs when attempting to log in on a system with Enhanced Security. If the login attempt times out or is terminated with a Control C, the following is seen: login: n1_1 Password: Login timed out malloc: Interrupted system call Connection closed by foreign host.• Fixes the problem of optimized programs printing incorrect values for long doubles.• A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability.• Corrects a regular expression performance problem in libc.• 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.• Increases the number of places of precision for formatted printing of long doubles.• Fixes a problem in which the vi editor core dumps when it finds invalid syntax during a substitute operation.• Restores correct behavior that existed on pre-V5.0 releases for ecvt() and fcvt(). Floating point exceptions and core dumps no longer occur when denormalized values are passed to ecvt() and fcvt().• Resolves issues with customer applications that experienced floating point exceptions and core dumps when passing denormalized values to ecvt() and fcvt() that subsequently caused INFORMIX databases to crash.• Fixes regular expression handling with non-default locale settings.
---------------------------	---

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

Patch 236.00 OSF505-268	Patch: Fixes a problem with the grep command State: Supersedes patch OSF505-010 (19.00) This patch fixes a problem with the grep command in which the options -p -v together do not produce any output.
Patch 238.00 OSF505-152	Patch: Fix for quotacheck command State: New This patch fixes a bug where quotacheck -v <filesystem> will report that it has fixed some quotas. If you keep running the command, it will keep reporting the exact same fixes.
Patch 242.00 OSF505X11-018	Patch: X server does not display windows properly State: New. Supersedes patches OSF505X11-019 (239.00), OSF505X11-015 (240.00) This patch corrects the following: <ul style="list-style-type: none">• Changes the X server to dynamically retrieve its vendor string information when running on COSIX64.• Fixes a memory leak in the X server that could occur when a client repeatedly created and destroyed buffers for the X Window System Multibuffering Extension (XmbufCreateBuffers/XmbufDestroyBuffers).• Fixes a problem where the X server does not display windows properly for the 128th and subsequent clients.
Patch 279.00 OSF505-217B	Patch: Support for activating temporary data logging State: New This patch provides support for activating temporary data logging on a mount point.
Patch 289.00 OSF505-224	Patch: Fix for pax and vdump problems State: Supersedes patches OSF505-012 (21.00), OSF505-077A (79.00), OSF505-155 (287.00) This patch corrects the following: <ul style="list-style-type: none">• Fixes a cpio hanging problem in the Japanese locales.• Fixes the following pax and vdump problems:<ul style="list-style-type: none">– The pax/tar command opens and truncates pre-existing files while extracting from an archive. This can cause problems when performing an update install.– The vdump command will backup automount symbolic links as files in a directory section. A restore of this link would then prevent automount from changing a directory file to a symbolic link file.• Fixes a problem where the tar -F (Fasttar) option ignores files named err but does not ignore files named errs and directories named SCCS and RCS.• This patch 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 (the following 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.

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

Patch 291.00 OSF505-174	Patch: Fixes a problem with dlclose State: Supersedes patch OSF505-085 (97.00) This patch corrects the following: <ul style="list-style-type: none">• Fixes a problem with the dlsym() routine. The problem was that dlsym() would perform a ring search when locating symbols in a library that was linked with the "-B symbolic" linker flag. The dlsym() search in this case should only be a depth search. With this fix, only the selected library and its dependencies will be searched. The search will not continue to the application and its dependencies.• Fixes a problem with dlclose() that prevented the Apache web server from running on V5.0A.
Patch 293.00 OSF505DX-017	Patch: Updates Netscape Communicator to Version 4.76 State: New This patch updates Netscape Communicator to Version 4.76 to fix missing default MIME types in Netscape Communicator Version 4.75.
Patch 296.00 OSF505-225	Patch: ksh problems occur in multi-byte Asian locales State: New. Supersedes patch OSF505-192 (294.00) This patch corrects the following: <ul style="list-style-type: none">• Fixes a possible handling problem with multibyte character boundary conditions in ksh script processing.• Fixes two ksh problems that occur in multi-byte Asian locales.

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

Patch 301.00 OSF505-237	<p>Patch: Fixes problems relating to the operation of hsg80</p> <p>State: Supersedes patches OSF505-036 (45.00), OSF505-037 (46.00), OSF505-035 (44.00), OSF505-073 (82.00), OSF505-101 (102.00), OSF505-133 (159.00), OSF505-075 (85.00), OSF505-098 (103.00), OSF505-145 (186.00), OSF505-066 (83.00), OSF505-244 (297.00), OSF505-196 (298.00), OSF505-172 (299.00)</p> <p>This patch corrects the following:</p> <ul style="list-style-type: none">• Fixes the following two problems in the I/O subsystem:<ul style="list-style-type: none">– Only the first byte of the HSZ serial number is checked.– The time allowed for the command timeout on AIT tape drives is increased to from 5 seconds to 5 minutes.• Fixes a problem in which a reboot will fail after hwmgr is used to delete or add devices.• Corrects a kernel memory fault caused by hwmgr.• When using the hwmgr -edit scsi command to make a non-shared SCSI device have a unique identifier, the SCSI device should be registered with the hardware management code as shared. Prior to this fix, the SCSI device was still being registered as non-shared.• Fixes a panic during a multi-node reboot. The panic has the following error message: panic: lock_write• Prevents an AdvFS Domain Panic from occurring during the boot process following a clu_add_member.• Fixes the following CAM disk problems that occur occasionally only during heavy IO:<ul style="list-style-type: none">– EPERM errors are reported to the application when a device is reopened.– A device may become unavailable to DRD and will failover even if there is a viable path to the device.• Fixes a problem such that when connectivity of a device is restored in a cluster environment, the state of the paths to the device may not be current. The problem symptoms will be one or more of the following:<ul style="list-style-type: none">– Member node hang for a minute or more.– Member node does not become a server for the device.– Persistent reservation not re-applied to the device.• Fixes a problem in 5.0A Initial Patch Kit where disks can become inaccessible on a cluster node with the following message: DRD barrier failed against 219 returned 60 (=ETIMEDOUT)• Fixes a problem in which the SCSI_MC_GENERIC-READ_ELEMENT_STATUS fails with an ioctl return status of -1 and "i/o error".• Fixes the inconsistencies 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.
----------------------------	---

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

Patch 301.00 continued	<ul style="list-style-type: none">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 LISTFixes a problem in which data can become corrupted on hardware configurations that use multiported parallel Fibre Channel storage arrays.Fixes problems relating to the operation of hsg80s.
Patch 307.00 OSF505-255	<p>Patch: Updates emx Fiber Channel driver to Revision 1.22</p> <p>State: Supersedes patches OSF505-053 (59.00), OSF505-141 (161.00), OSF505-140 (215.00), OSF505-227 (302.00), OSF505-235 (303.00), OSF505-195 (304.00), OSF505-142 (305.00)</p> <p>This patch corrects the following:</p> <ul style="list-style-type: none">Updates the emx Fiber Channel driver to Revision 1.22 which corrects a Data Error that is seen when running with the latest Emulex firmware. This error corrupts data when reading from the disk. This revision also fixes an error that causes performance degradation.This patch fixes the following DE600/DE602 10/100 Ethernet adapter problems:<ul style="list-style-type: none">The primary CPU may appear hung on networks where switches send Flow Control Pause frames if they become overloaded.Transmit timeout messages appearing in the console log due to the driver timing out a frame.Provides support for the DEGPA-TA (1000BaseT) Gigabit Ethernet device.Fixes a problem where cascaded switches can hang the system at failover time.Fixes kernel build failures due to an undefined ss_sched function.Addresses two problems with the ee driver for DE60x Ethernet cards. These problems affect all Tru64 systems containing ee cards:<ul style="list-style-type: none">A fix for a race condition where the card could stop receiving packets from the network under rare circumstances.A fix for the lan_config user options -x and -s.Provides the device driver support for 3DLabs Oxygen VX1 graphics adapter.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.

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

Patch 309.00 OSF505X11-016	Patch: Fixes a memory leak in the X server State: Supersedes patch OSF505X11-005 (12.00) This patch corrects the following: <ul style="list-style-type: none">• Fixes a problem where, on systems with a PowerStorm 4D10T (ELSA Gloria Synergy, SN-PBXGK-BB) graphics card or a PCI To Ethernet/Graphics Combo Adapter (3X-DEPVD-AA), sometimes lines and images are not drawn correctly in scrolled windows.• Fixes synchronization and drawing problems in the X server for the PowerStorm 4D10T (ELSA Gloria Synergy, SN-PBXGK-BB) graphics card.• Fixes a memory leak in the X server on systems with a PowerStorm 4D10T (ELSA Gloria Synergy, SN-PBXGK-BB) graphics card that could occur when a client repeatedly created and destroyed buffers for the X Window System Multibuffering Extension (XmbufCreateBuffers/XmbufDestroyBuffers).
Patch 312.00 OSF505X11-016	Patch: Security (SSRT1-19U) State: New. Supersedes patch OSF505-214 (310.00) A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability.
Patch 315.00 OSF505X11-017	Patch: Corrects blocks of erroneous pixels State: New. Supersedes patch OSF505X11-013 (313.00) This patch provides the Xserver library for the new 3Dlabs OXYGEN VX1 PCI graphics card. This patch corrects blocks of erroneous pixels left behind when dragging CDE Application Manager icons on the desktop.
Patch 317.00 OSF505X11-007	Patch: X server grows excessively when accessing fonts State: New This patch fixes a problem where the X server can grow excessively when accessing certain fonts.
Patch 319.00 OSF505-220A	Patch: Fix for EVM daemon, evmd State: Supersedes patch OSF505-013A (22.00) This patch corrects the following <ul style="list-style-type: none">• Fixes the following EVM problems on some Alpha EV6 systems:<ul style="list-style-type: none">– evmshow and the event viewer will display timestamps that are incorrect by one hour for binlog events when Daylight Savings Time is in effect.– When a binlog event is being displayed on a system located in a different time zone from the system that originally posted the event, the time may be displayed as local time for the posting system. This is inconsistent with the way time is displayed by other utilities, including DECEvent and Compaq Analyze.• Fixes two problems with the EVM daemon, evmd. The EVM daemon will crash under the following conditions:<ul style="list-style-type: none">– There are blank lines in the /etc/rc.config file.– The EVM daemon tries to retrieve events using a cluster local memory channel. This would happen when executing a command such as evmget -h systemA-mc0 evmshow.

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

Patch 321.00 OSF505-220B	Patch: Static library fix for libevm State: Supersedes patch OSF505-013B (71.00) This patch corrects the following <ul style="list-style-type: none">• Fixes the following EVM problems on some Alpha EV6 systems:<ul style="list-style-type: none">– evmshow and the event viewer will display timestamps that are incorrect by one hour for binlog events when Daylight Savings Time is in effect.– When a binlog event is being displayed on a system located in a different time zone from the system that originally posted the event, the time may be displayed as local time for the posting system. This is inconsistent with the way time is displayed by other utilities, including DECevent and Compaq Analyze.• Fixes two problems with the EVM daemon, evmd. The EVM daemon will crash under the following conditions:<ul style="list-style-type: none">– There are blank lines in the /etc/rc.config file.– The EVM daemon tries to retrieve events using a cluster local memory channel. This would happen when executing a command such as evmget -h systemA-mc0 evmshow.
Patch 326.00 OSF505-164	Patch: New JJ printcap parameter State: Supersedes patches OSF505-017 (26.00), OSF505-092 (101.00), OSF505-104 (155.00), OSF505-144 (157.00) This patch corrects the following: <ul style="list-style-type: none">• Fixes the following printing problems:<ul style="list-style-type: none">– When using the I18N ya option, the queue daemon filters will terminate after 32 jobs.– Under certain circumstances, print jobs are terminated when printing to certain printers that are connected to a DECserver through TCP/IP.– The read-backs for remote connections cause an additional 2-second time out which may cause a job-submit failure on the job-number wraparound.– A user is unable to delete a print job from a remote system with a hostname greater than 32 characters because the hostname was truncated.– When a TCP/IP connection fails, the retry algorithm would take longer to print jobs due to a long retry interval.– A timing hole during lpd last-job completion and shutdown needed to be closed.– It was not possible to print to the lpd queue using Windows 2000.• Corrects a problem in which, under certain conditions, unnecessary error messages are written to the lpr.log file.• 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).
Patch 328.00 OSF505DX-014	Patch: dop tool causes segmentation fault State: New This patch fixes a problem in which the dop tool would cause a segmentation fault when a non-root user entered the root password.

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

Patch 330.00 OSF505CDE-005	Patch: Fixes a problem on multi-head systems State: 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 332.00 OSF505-109	Patch: ATM setup script fails when configuring ELAN State: New This patch fixes a problem of the ATM setup script failing when configuring an ELAN if the lane subsystem is not loaded.
Patch 334.00 OSF505-219	Patch: Corrects problem with inetd State: New This patch corrects a problem with inetd which could result in its termination without notice and without a core file.
Patch 336.00 OSF505-230	Patch: OSF505-230 State: 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 338.00 OSF505-240	Patch: Kernel memory fault in systems running RMS software State: New This patch fixes a kernel memory fault and invalid memory ifetch panic which can occur in systems running Quadrics' RMS software.
Patch 340.00 OSF505-176	Patch: Fix for newgrp command failure State: New This patch corrects the problem where newgrp(1) fails if the file /etc/group contains multiple lines for one group.
Patch 342.00 OSF505DX-015	Patch: Fixes a problem in diskconfig State: New This fixes a problem in diskconfig where partitions with an offset and size of zero cannot be selected. It also fixes a problem where overlapping partitions cannot be adjusted if the existing partitions are not in alphabetical order.
Patch 348.00 OSF505-177	Patch: Security (SSRT0672U) State: New A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability.
Patch 350.00 OSF505-208	Patch: Fixes automount handling of the nogrpid option State: Supersedes patch OSF505-022 (31.00) This patch corrects the following: <ul style="list-style-type: none">• Prevents the message "nfcst: select: Invalid argument" message from appearing in the daemon.log when the server is not available.• Changes the "trymany: servers not responding: RPC: Unable to receive" message to an informational rather than an error message.• Fixes the automount handling of the nogrpid option.
Patch 352.00 OSF505-154	Patch: Fixes a problem in rpc.lockd State: New This patch fixes a problem in rpc.lockd where the FCNTL () function fails to lock NFS mounted directories.

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

Patch 354.00 OSF505DX-013	Patch: Security (SSRT0654U, SSRT0662U, SSRT0663U) State: New A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability.
Patch 357.00 OSF505-242	Patch: Upgrades sys_check utility to version v120 State: Supersedes patches OSF505-131 (202.00), OSF505-190 (355.00) This patch corrects the following: <ul style="list-style-type: none">• Upgrades sys_check utility to version 119 and provides the following changes:<ul style="list-style-type: none">– Utilizes Compaq Analyze when available.– Utilizes storages new cliscript tool in place of hszterm.– Provides an updated ASU section.• Upgrades sys_check to V120.• Fixes errors generated by syscheck when NFS is not configured.
Patch 359.00 OSF505DX-012	Patch: Fix for bindconfig State: New This patch fixes the problem of OutOfOrder hide stack trace, which occurs when invalid domain name or invalid server information is entered during bindconfig.
Patch 361.00 OSF505-201	Patch: Replaces declarations of wcostok and wcsftime State: New This change replaces declarations of wcostok() and wcsftime() interfaces with the correct declarations defined in ISO/IEC 9899:1990/Amendment 1:1994(E).
Patch 363.00 OSF505CDE-006	Patch: Fix for dtpad State: New This patch fixes a problem where, if dtpad cannot allocate enough memory, it will exit and leave a zero-length file in place of the file being edited.
Patch 365.00 OSF505-157	Patch: Corrects a stack overflow panic State: 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 367.00 OSF505-254	Patch: Fix for ksh hang State: New This patch fixes a problem where the Korn shell (ksh) could hang if the user pasted a large number of commands to it when it was running in a terminal emulator window (such as an xterm).
Patch 371.00 OSF505-173	Patch: Fix for ATM signalling problem State: New. Supersedes patch OSF505-024 (33.00) This patch corrects the following: <ul style="list-style-type: none">• Fixes a problem in which the system may panic with the error message "simple lock: time limit exceeded" when running ATM.• Fixes a problem of ATM signalling going into "connection released" after a system reboot.

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

Patch 373.00 OSF505-193	Patch: Corrects memory leak in XTI socket code State: New This patch corrects a memory leak in the XTI socket code.
Patch 375.00 OSF505-158	Patch: Fix for fsx State: New This patch corrects a problem in which fsx would disregard the -s flag.
Patch 377.00 OSF505-182	Patch: Fix for data structure inconsistencies State: New This patch prevents a panic on TurboLaser systems with a DE600 in pci slot 0. Mis-identification of the DE600 in pci slot 0 causes data structure inconsistencies. 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 379.00 OSF505-238	Patch: Fixes possible EVM configuration problems State: New This patch fixes possible EVM configuration problems during a cluster rolling upgrade.
Patch 383.00 OSF505-189	Patch: Fixes linker (ld) problems State: Supersedes patches OSF505-029 (38.00), OSF505-213 (380.00), OSF505-194 (381.00) This patch corrects the following: <ul style="list-style-type: none">• Linking large applications with -om -call_shared with very large numbers of external symbols sometimes failed to link.• Fixes a problem where the linker defined symbol _fpdata would end up being undefined if it was referenced by a program but not used by the linker.• Fixes two problems in the linker where it would erroneously report "multiply defined symbol" errors or "unresolved symbol" errors.<ul style="list-style-type: none">– Modifies the linker's symbol resolution to enable it to recognize when a reference to a symbol defined in a shared library is replaced by a symbol defined in an object file or archive.– Modifies the linker to cause it to rescan shared libraries before reporting unresolved symbols.• Fixes two errors that occur when using the -f switch with the linker (ld):<ul style="list-style-type: none">– Using the -f switch produces link errors.– Any unsupported switch beginning with -f gets interpreted to mean -f.
Patch 385.00 OSF505-246	Patch: Security (SSRT1-15, SSRT0713U) State: New A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability.

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

Patch 387.00 OSF505-179	Patch: rdist utility causes segmentation faults State: New This patch corrects a problem in the rdist utility which was causing segmentation faults on files with more than one link.
Patch 389.00 OSF505-160	Patch: KMF occurs while using tablet instead of mouse State: Supersedes patch OSF505-049 (57.00) This patch corrects the following: <ul style="list-style-type: none">• Fixes a "lock_terminate: lock held" panic when deleting a process group.• Fixes a kernel memory fault which occurs while using a tablet instead of a mouse.
Patch 391.00 OSF505-229	Patch: Fixes DS10/DS20 performance problems State: New This patch fixes DS10/DS20 performance problems introduced with the i2c driver by using thread blocking, rather than event_timeout() and DELAY().
Patch 393.00 OSF505-170	Patch: Fix for system panic State: New This patch fixes a problem in which the system may panic with the panic string "Unaligned kernel space access from kernel mode".
Patch 396.00 OSF505-186	Patch: Security (SSRT0664U) State: New. Supersedes patch OSF505-149 (394.00) This patch corrects the following: <ul style="list-style-type: none">• A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability.• Corrects a problem with the ftpd daemon which could result in PC ftp clients hanging when transferring some files in ASCII mode.
Patch 403.00 OSF505-207	Patch: CDFS media burned in 2001 shows the wrong dates State: New CDFS media burned in 2001 shows the wrong dates.
Patch 405.00 OSF505-212	Patch: Fix for joind State: New This patch corrects a problem with joind which caused it to respond to certain client dhcp requests via the wrong port.

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

Patch 407.00 OSF505-200	Patch: Potential system crash when accessing the FDI floppy State: Supersedes patches OSF505-074 (84.00), OSF505-166 (217.00) This patch corrects the following: <ul style="list-style-type: none">• Corrects a hardware probe time hang that maybe encountered when booting.• Compaq has determined in laboratory testing that there is a theoretical possibility that during read and write operations to the floppy disk on DS10, DS10L and ES40 AlphaServers and VS10 and XP900 AlphaStations, a single byte of data may be inaccurately read or written without notice to the user or system. The potential for this anomaly exists only if floppy data read and write operations are attempted while there is extremely heavy traffic on these Alpha systems' internal input/output busses. Although Compaq has observed the anomaly only in laboratory tests designed to create atypical system stresses, including almost constant use of the floppy disk drive, we are supplying this patch to address this potential issue.• Corrects a potential system crash when accessing the FDI floppy.
Patch 409.00 OSF505CDE-007	Patch: CDE window manager loops when creating workspaces State: Supersedes patch OSF505CDE-004 (209.00) This patch corrects the following: <ul style="list-style-type: none">• Fixes a problem in which the Window Manager (dtwm) intermittently hangs on a system which uses multiple displays.• Fixes a problem where the Common Desktop Environment (CDE) window manager loops or aborts when creating and deleting workspaces or when displaying the CDE Window List.
Patch 411.00 OSF505-247	Patch: Security (SSRT0713U) State: New A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability.
Patch 414.00 OSF505-180	Patch: sysman utility reports syntax error State: New. Supersedes patch OSF505-222 (412.00) This patch corrects the following: <ul style="list-style-type: none">• Fixes a problem with the installation process rejecting a subset name with an underscore character on a V5.0A system (specifically, when a user was trying to install the IBM MQSeries Documentation Base subset, MQS_HTML_PUBS).• Fixes an issue with the sysman utility reporting a syntax error on a V50A system with Multimedia_Service.

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

Patch 418.00 OSF505-211	<p>Patch: Fixes problems in the Compaq C compiler</p> <p>State: Supersedes patches OSF505-021 (30.00), OSF505-129 (198.00)</p> <p>This patch corrects the following:</p> <ul style="list-style-type: none">• A virtual memory exhausted error when compiling the Open Source encryption library OpenSSL.• An optimizer problem in loop unrolling that caused an incorrect result under certain conditions.• Various compiler crashes under certain conditions.• An optimizer problem that caused the exception handling programs in Chapter 11 of the Programmer's Guide to fail.• An optimizer problem that caused a Perl validity test to fail when using a long double NaN.• An optimizer problem that caused the wrong answer to be produced for a program involving tail recursion.• A problem in bounds checking that caused a compilation to fail with a virtual memory exceeded error.
Patch 420.00 OSF505-293A	<p>Patch: Fix for parallel processing support library</p> <p>State: New</p> <p>This patch fixes a problem in the parallel processing support library (libots3) that caused incorrect run-time results for an OpenMP program.</p>
Patch 422.00 OSF505-293B	<p>Patch: Fix for libots3 static library</p> <p>State: New</p> <p>This patch fixes the following problems:</p> <ul style="list-style-type: none">• A problem in the Compaq C compiler in bounds checking that caused a compilation to fail with a virtual memory exceeded error.• A problem in the parallel processing support library (libots3) that caused incorrect run-time results for an OpenMP program.
Patch 426.00 OSF505-262B	<p>Patch: Fix for bad frag free list AdvFS panic</p> <p>State: New</p> <p>This patch modifies AdvFS kernel code and several utilities. AdvFS will no longer panic with the following error:</p> <p>ADVFS EXCEPTION : panic cpu(0) : bad frag free list</p> <p>The code is modified so that during frag allocation when AdvFS determines that the frag group header's free list has been corrupted, it stops using it and marks it BAD. It is then removed from the free list so no more allocations can take place and no deallocations are performed. The verify, shfragbf, and vfragpg programs are modified to report BAD frag groups.</p>

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

Patch 428.00	Patch: Security (SSRT0676U SSRT0700U)
OSF505-300	State: Supersedes patches OSF505-040 (91.00), OSF505-102 (142.00), OSF505-091 (143.00), OSF505-088 (144.00), OSF505-093 (145.00), OSF505-134 (146.00), OSF505-123 (148.00), OSF505-151 (280.00), OSF505-206 (281.00), OSF505-232 (282.00), OSF505-231 (283.00), OSF505-245 (284.00), OSF505-027 (36.00), OSF505-019 (28.00), OSF505-020 (29.00), OSF505-034 (43.00), OSF505-041 (49.00), OSF505-047 (55.00), OSF505-048 (56.00), OSF505-050 (58.00), OSF505-007 (16.00), OSF505-008 (17.00), OSF505-009 (18.00), OSF505-065 (93.00), OSF505-079 (88.00), OSF505-083 (94.00), OSF505-084 (96.00), OSF505-114 (135.00), OSF505-126 (136.00), OSF505-138 (137.00), OSF505-094 (138.00), OSF505-103 (139.00), OSF505-112 (141.00), OSF505-039 (48.00), OSF505-067 (77.00), OSF505-111 (190.00), OSF505-054 (60.00), OSF505-076 (89.00), OSF505-187 (243.00), OSF505-218 (244.00), OSF505-183 (245.00), OSF505-223 (246.00), OSF505-233 (247.00), OSF505-253 (248.00), OSF505-159 (249.00), OSF505-148 (250.00), OSF505-236 (251.00), OSF505-203 (252.00), OSF505-215 (254.00), OSF505-162 (255.00), OSF505-150 (256.00), OSF505-234 (257.00), OSF505-249 (258.00), OSF505-197 (259.00), OSF505-156 (260.00), OSF505-198 (261.00), OSF505-226 (262.00), OSF505-188 (263.00), OSF505-262 (264.00), OSF505-263 (265.00), OSF505-217A (266.00), OSF505-181 (267.00), OSF505-239 (268.00), OSF505-147 (269.00), OSF505-185 (270.00), OSF505-169 (271.00), OSF505-248 (272.00), OSF505-199 (273.00), OSF505-175 (274.00), OSF505-251 (275.00), OSF505-205 (277.00), OSF505-202 (286.00), OSF505-216 (416.00), OSF505-262A (424.00)
	This patch corrects the following:
	<ul style="list-style-type: none">• Fixes a problem where the operating system only looks in slot 0 for the primary CPU.• Fixes a problem that causes inconsistencies in the floating point registers whereby the flag fields <code>nxm_fp_owned</code> are overwritten with 0s.• Fixes "can_replace: slot replacement mismatch" panics which can occur when running multithreaded applications.• Fixes a problem in which metadata buffers are being written asynchronously instead of on a delayed basis.• Fixes a problem in which the POSIX interval timer is not resilient to clock slowdown, caused either by NTP or by a backward change of the clock.• Fixes a problem where, if the size of the message queue was increased, writers to the queue that were blocked would not wake up for processing.• Fixes a problem where the system appears to hang. A child process is holding a lock too long and preventing other processes from doing work.• Fixes an "unaligned kernel space access from kernel mode" panic when doing a malloc from <code>kmembucket 26, 896 byte bucket</code>. The faulting virtual address will be the lock signature for <code>thread_deallocate()</code>.• Fixes a "simple_lock time limit exceeded" panic due to an SMP race condition in namecache.• Fixes a bug such that, when user <code>-k</code> is issued on a dismounted NFS mount point in which a process is running, a hang will occur.• Fixes a race condition in the UBC code where a lookup is done on a page being invalidated (freed).• Fixes a hang or <code>simple_lock_state_violation</code> panic in <code>biodone</code>.

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

Patch 428.00 continued	<ul style="list-style-type: none">• Fixes a system panic in <code>cfs_unmount</code>. The panic string is: <code>cfs_unmount: panic("VFS_UNMOUNT failed ")</code>. This is caused by a race condition in <code>ubc_invalidate()</code> where pages could be missed if they transition from the clean list to the dirty list.• Fixes "simple_lock: time limit exceeded" system panic either from <code>cache_lookup()</code> or <code>cache_enter()</code>. This is caused by the namecache LRU list getting corrupted.• Fixes a binary compatibility problem for the four system calls <code>sendmsg</code>, <code>nsendmsg</code>, <code>recvmsg</code>, and <code>nrecvmsg</code> were not preserved between V4.0x and V5.x releases.• This patch fixes two panics that have the following error messages: <code>simple_lock: time limit exceeded</code> <code>simple_lock: lock already owned by cpu</code>• Corrects a problem where there is a potential for a system panic in routine <code>sbflush()</code> if there is an attempt to flush a socket buffer while it is locked by another thread.• Fixes panics and memory inconsistencies in <code>setuid/setgid</code>.• This is a kernel patch that addresses a binary compatibility problem seen with four networking system calls: <code>sendmsg</code>, <code>osendmsg</code>, <code>recvmsg</code>, and <code>orecvmsg</code>. In certain cases, executables compiled on other versions of Tru64 UNIX will not work correctly when using these system calls.• Fixes a panic in the UFS filesystem which has the following error message: <code>blkfree: freeing free block</code>• Fixes a system hang that can occur during an NFS operation on a system running granularity hints.• Fixes a problem where the output of a <code>ps</code> command, the <code>PAGEIN</code> column, reports 0 for all processes.• Fixes an AdvFS problem where, under the right conditions, a Kernel Memory Fault panic can occur while writing to an Atomic Data Logging file.• Corrects a problem whereby under certain unlikely conditions, a b-tree index for a directory could become corrupted.• Fixes a kernel memory fault in <code>u_anon_faultpage()</code> when it accesses the backing object for the anonymous page.• Fixes a situation in which adding swap space results in system instability.• Fixes a hang seen while running <code>collect</code> and the <code>vdump</code> utility.• Prevents the hang in <code>tok_wait</code> from occurring.• Fixes an issue with lightweight wiring of pages and shared memory regions.• Fixes inaccuracy problems when using <code>setrlimit/getrlimit</code> with a threaded application.• Fixes a system hang caused by <code>netisr</code> queue inconsistencies due to a race condition that is primarily encountered by third party drivers and layered products that call <code>schednetisr_nospl()</code>.• Fixes a problem where threads can hang in <code>x_load_in-mem_xtnt_map()</code>.
---------------------------	--

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

Patch 428.00 continued	<ul style="list-style-type: none">• Fixes a timing window where flushing data to disk can be incomplete when a system is going down, if more than one thread calls <code>reboot()</code> without first going through <code>shutdown</code>, <code>/sbin/reboot</code>, or <code>/sbin/halt</code>.• Fixes a problem in which the wrong status was returned from EEROM read.• Adds a tunable parameter <code>non_preempt_limit</code> into the generic section for <code>sysconfig</code>. The parameter is used to debug certain long running and non-preemptible kernel threads on a system.• Fixes a hang in the UFS filesystem.• Fixes a kernel memory fault when writing to <code>/proc</code>, while <code>anon_rss_enforce</code> is set to 2.• A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability.• Fixes a problem in UFS. The <code>O_SYNC</code> does not work properly causing the inode update to fail on a synchronous write.• Updates to an AdvFS file via <code>directIO</code> may not correctly merge the old data and the new data if 1) the write is to the frag and 2) the write does not completely overwrite all the old data. This fixes that symptom.• Fixes a problem that causes Tarantella Enterprise 1.41 not to install on Tru64 UNIX.• Fixes a potential problem flushing data to disk when using data logging with sparse files.• Prevents <code>stat()</code>, <code>lstat()</code>, <code>fstat()</code>, <code>statfs()</code>, <code>fstatfs()</code>, <code>getmntinfo()</code>, and <code>getfsstat()</code> from returning <code>E_OVERFLOW</code> errors for programs compiled on Tru64 UNIX V4.0n or earlier.• Fixes a performance problem in AdvFS. Checksum calculation loops were removed to speed up performance.• 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 <code>direct I/O</code>. 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:<ul style="list-style-type: none">– An application writes to a file using AdvFS <code>direct I/O</code> and the file had previously been opened for normal <code>I/O</code> (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 <code>direct I/O</code> 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 <code>direct I/O</code> and remains open for <code>direct I/O</code>, the problem does not exist. Applications that use <code>direct I/O</code>, such as Oracle, could be affected.• Fixes a problem where the <code>setgid</code> bit of a directory was not being set when created, if its parent directory has the <code>setgid</code> bit set.
---------------------------	--

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

Patch 428.00 continued	<ul style="list-style-type: none">• Fixes an issue with some remote ioctls for tape/changer drivers not working in a cluster.• Modifies advfs kernel code and several utilities. AdvFS will no longer panic with the following error: ADVFS EXCEPTION : panic cpu(0) : bad frag free list. The code is modified so that during frag allocation when advfs determines that the frag group header's free list has been corrupted, it stops using it and marks it BAD. It is then removed from the free list so no more allocations can take place AND no deallocations are performed. The verify, shfragbf and vfragpg programs are modified to report BAD frag groups.• Fixes several virtual memory algorithms related to the allocation and freeing of pages within the kernel.• Provides support for activating temporary data logging on a mount point.• 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.• 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.• Fixes a kernel memory fault from ufs_mount().• Resolves hang-like behavior when LSM volumes are used to create AdvFS domain volumes. The default preferred IO byte transfer size may be too large and needs to be set lower.• This patch corrects an AdvFS panic which can occur during a rmfset operation with the panic string: rbf_delete_int: can't find bf attributes• Fixes a "u_anon_free: page busy" panic.• Fixes a kernel memory fault from quotaUndo.• Fixes panics which can occur if a signal is sent to a multi-threaded task in which one or more threads are calling exit() or exec().• Fixes a problem where under certain circumstances, a Tru64 UNIX system can panic with the string: "lock_write: simple lock owned" in the if_slowtimo() routine.• Fixes a problem that has the potential to cause a noticeable performance degradation in the Cluster File System on systems that perform large writes. This patch is to prevent a deadlock in NFS over TCP that could occur if the client is not responding properly. The hang will be seen in the nfs tcp threads in rrok3free().• Prevents an sbdrop panic from occurring.• Fixes a panic in in_pcbfree() when NFS is implemented over TCP.• Corrects a problem which could cause the system to spend excessive time in the internet checksum routine, resulting in a degradation of system performance.• Corrects the problem with write errors seen on soft mounted NFS filesystems. The error received is: NFS3 RFS3_WRITE failed for server ncinfo: RPC: Server can't decode arguments• Increases speed of large NFS client I/O.
---------------------------	--

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

Patch 428.00 continued	<ul style="list-style-type: none">• Prevents a possible NFS over TCP hang. NFS TCP threads will be blocked in sosbwait() causing the system to appear to be hung.• Fixes a problem where some network based multimedia applications will cause a kernel memory fault when exiting.• Corrects a problem where a directory entry may be attempted to be changed to "." and the code checks for this prevents it from happening.• 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.• Corrects a problem where a race condition in NFS can result in a kernel memory fault.• Fixes a problem where threads can hang while renaming files on NFS mounted filesystems.• Fixes a panic which can occur on a V5.0A TruCluster system.• Corrects the problem with write errors seen on soft mounted NFS filesystems. The error received is: "NFS3 RFS3_WRITE failed for server ncinfo: RPC: Server can't decode arguments". This is the second part of the fix for this issue.• Fixes a kernel memory fault panic in anon_getpage(), _ms_free(), and locking issues regarding the vm_kanon hash list. Incorrect locking around the vm_kanon hash list searching and removal could lead to kernel memory faults, simple lock timeouts, or corrupted kernel data.• fFixes a "simple_unlock: lock not owned by cpu" panic in the biodone routine.
Patch 430.00.00 OSF505-243	<p>Patch: Fix for kernel memory fault on EV6 systems</p> <p>State: Supersedes patches OSF505-261 (322.00), OSF505–303 (324.00)</p> <p>This patch corrects the following:</p> <ul style="list-style-type: none">• Fixes a problem that can cause a simple lock timeout or a kernel memory fault on EV6 systems using the itpsa driver.• Fixes a problem with some slower tape devices serviced by the itpsa driver by lengthening the timeout value used.• Fixes a kernel memory fault that can occur when performing disk I/O.

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 28.00, 50.00, 52.00	New
Patches 2.00, 4.00, 12.00, 21.00, 8.00, 29.00, 30.00, 31.00	Superseded by Patch 33.00
Patches 3.00, 13.00, 6.00, 7.00, 9.00, 10.00, 11.00, 24.00, 5.00, 1.00, 14.00, 15.00, 16.00, 17.00, 19.00, 26.00, 34.00, 35.00, 36.00, 37.00, 38.00, 39.00, 40.00, 41.00, 42.00, 43.00, 44.00, 45.00, 46.00, 48.00	Superseded by Patch 54.00

Table 3–2: Summary of TruCluster Patches

Patch IDs	Abstract
Patch 23.00 TCR505-019	<p>Patch: Fixes a problem with the Memory Channel API</p> <p>State: New</p> <p>This patch fixes a problem with the Memory Channel API, whereby a node crashes holding an mc-api lock. Under certain circumstances the lock will not be released after the node crashes.</p>
Patch 28.00 TCR505-027	<p>Patch: Fixes a problem in CFS/NFS</p> <p>State: New</p> <p>This patch fixes a problem in CFS/NFS. NFS permissions are not handled properly in CFS.</p>

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

Patch 33.00 TCR505-031	Patch: Fix for MC2 vhub cluster panic State: Supersedes patches TCR505-006 (2.00), TCR505-002 (4.00), TCR505-014 (12.00), TCR505-021 (21.00), TCR505-008 (8.00), TCR505-039 (29.00), TCR505-043 (30.00), TCR505-032 (31.00) This patch corrects the following problems: <ul style="list-style-type: none">• Fixes a system panic that can be caused by Memory Channel errors occurring when the system is under heavy load.• Improves cluster communication performance including file system mount times.• Corrects problems seen when both a member is leaving and joining the cluster at the same time.• Corrects problems with loss of quorum in a cluster. Once the quorum is lost, the member may panic with the panic string: QNX DISK: yeilding to foreign owner with quorum.• If lockmode has been set to 4, booting an MC2 vhub cluster generates the following panic on the second node booting: simple_lock: uninitialized lock panic (cpu 0): simple_lock: uninitialized lock• Eliminates double failure panics in vhub configurations and removes rmerror_int diagnostic messages.• Fixes a problem in ICS where ring_recv() does not properly handle a change in channel numbers. The fix will, in turn, improve validation of the connection structure on node joins.• Corrects a problem in which a loss of the cluster heartbeat could cause a member to panic with "CNX QDISK: Yielding to foreign owner with quorum".• Prevents a kmf (kernel memory fault) panic that can occur when a node is joining the cluster.
Patch 50.00 TCR505-045	Patch: Fix for system panic State: New This patch fixes a panic which can occur on a V5.0A TruCluster system.
Patch 52.00 TCR505-042	Patch: Fix for cluster node crash State: New This patch fixes a problem where a cluster node will crash on boot because CNX could not register seqdisk callback.

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

Patch 54.00 TCR505-053	<p>Patch: Security (SSRT0691U)</p> <p>State: Supersedes patches TCR505-009 (3.00), TCR505-018 (13.00), TCR505-003 (6.00), TCR505-007 (7.00), TCR505-010 (9.00), TCR505-012 (10.00), TCR505-013 (11.00), TCR505-023 (24.00), TCR505-004 (5.00), TCR505-005 (1.00), TCR505-015 (14.00), TCR505-024 (15.00), TCR505-020 (16.00), TCR505-016 (17.00), TCR505-017 (19.00), TCR505-011 (26.00), TCR505-046 (34.00), TCR505-028 (35.00), TCR505-041 (36.00), TCR505-040 (37.00), TCR505-044 (38.00), TCR505-035 (39.00), TCR505-033 (40.00), TCR505-029 (41.00), TCR505-030 (42.00), TCR505-036 (43.00), TCR505-038 (44.00), TCR505-026 (45.00), TCR505-025 (46.00), TCR505-034 (48.00)</p> <p>This patch fixes the following:</p> <ul style="list-style-type: none">• Delivers a new stripped <code>clu_genvmunix</code> and several fixes to the cluster rolling upgrade procedure.• Problem seen when running <code>clu_upgrade preinstall</code> commands on certain multi-CPU systems. Numerous error messages similar to the following are seen: *** Error *** Could not create: <code>ocolsocols/Old..ocols</code> If you see this problem enter a <code>Ctrl/C</code> and rerun the <code>clu-upgrade preinstall</code> command.• Fixes a situation which has caused a node panic with the following message: SIMPLE_LOCK: TIME LIMIT EXCEEDED PANIC ON SHARED TAPE• Solves a problem with booting and shutting down cluster nodes while using a tape (or changer) device in a 5.0A cluster.• Fixes a problem where a mount command will hang after DRM has restored the path to an HSG80 storage volume.• Fixes a problem where a path will fail after DRM has restored the path to an HSG80 storage volume.• This patch fixes a problem where on a cluster node, if a new device is detected by a HW scan while the cluster is running, one of the following situations can occur:<ul style="list-style-type: none">– Only one node will be able to use the device; if the device is Fibre Channel.– There is a small risk for data inconsistencies on parallel SCSI device on a shared bus if the node subsequently loses quorum.• Provides the DRD portion of a fix to prevent an AdvFS Domain Panic from occurring during the boot process following a <code>clu_add_member</code>.• Fixes a problem where on a cluster node, if a SCSI bus reset occurs, when there is a loss of quorum, the DRD will be blocked on tape devices.• Fixes a kernel memory fault panic in routines <code>cfstok_find_held_tok</code>. This is caused when the very first action of a new allocated thread is a lookup in an NFS filesystem of ".".• Fixes a problem where mounts that return "ESTALE" may loop forever. Prevents a KMF panic from occurring when an AdvFS mount is attempted without a fileset being specified.• Provides the CFS/CMS portion of a fix to prevent an AdvFS Domain Panic from occurring during the boot process following a <code>clu_add_member</code>.
---------------------------	---

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

Patch 54.00 continued	<ul style="list-style-type: none">• Corrects a problem with cluster members panic with a "kernel memory fault" when either running <code>sys_check</code> or multiple <code>cfsmgr</code> commands.• Provides performance enhancements for CFS.• Prevents a "request_internal: client already had token" panic from occurring when nodes are leaving and joining the cluster.• Prevents a <code>cfsdb_assert</code> panic from occurring in the CFS block reserve code. The system is most likely running process accounting that receives this type of panic.• A potential security vulnerability has been discovered, where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. Compaq has corrected this potential vulnerability.• Fixes several problems, including addressing the need for IOCTL for remote DRD, adding clean up for failed remote closes for non-disks, fixing error returns on failed tape/changer closes, and fixes to tape deadlock experienced in netbackups.• Fixes an issue with a tape/changer giving back busy on open if a close from a remote node failed.• Fixes a problem in which I/O to an hsg80 can hang.• Fixes a problem with a cluster-as-NFS-client, in which there is a potential race where a CFS client node may not correctly timeout its cached data for a given file. Thus, processes accessing the given file, on that particular cluster member, may not see changes made to the file via the NFS server, or other NFS clients.• Fixes the following two TruCluster problems:<ul style="list-style-type: none">– 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.– A cluster member cannot boot under specific hardware setup. The CFS mount fails because of the PR flag is not cleaned up.• Fixes a problem in which data can become corrupted on hardware configurations that use multiported parallel Fibre Channel storage arrays. It also fixes a problem in which shared tapes will incorrectly indicate that they are busy.• Provides performance enhancements for copying large files (files smaller than the total size of client's physical memory) between a CFS client and server within the cluster.• Corrects a problem in which a cluster member can panic with the panic string "<code>cfsdb_assert</code>" when a NFS V3 TCP client attempts to create a socket using <code>mknod(2)</code>.• Corrects a problem in which a cluster member will panic with the patch string "<code>lock_terminate: lock held</code>" from <code>cinactive()</code>.• Fixes a problem in CFS. CFS stops serving lock requests resulting in a process hang.
--------------------------	---

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

Patch 54.00 continued	<ul style="list-style-type: none"><li data-bbox="552 193 1351 262">• Prevents possible file inconsistencies that can occur during a CFS/NFS race condition.<li data-bbox="552 262 1351 367">• Fixes a hang seen while running collect and the vdump utility. This patch prevents the hang in tok_wait from occurring. This also prevents a cfsdb_assert panic that contains the following message: Assert Failed: (tcbp->tcb_flags & TOK_GIVEBACK) == 0<li data-bbox="552 409 1351 476">• Fixes a problem where booting several nodes in a cluster simultaneously which could cause a KMF panic to occur.
--------------------------	---
