Tru64 UNIX Version 4.0F and TruCluster Software Version 1.6

Patch Summary and Release Notes for Patch Kit-0008

August 2003

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

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

Hewlett-Packard Company
Palo Alto, California

None of Compaq, HP, or any of their subsidiaries shall 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

Tables

About This Manual

This manual contains information specific to Patch Kit-0008 for the Tru64 UNIX™ Version 4.0F operating system and TruCluster™ Version 1.6 Software Products. It provides a list of the patches contained in each kit and describes any information you need to know about 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 anyone who installs and removes the patch kit and who manages patches after they are installed.

Organization

This manual is organized as follows:

Chapter 1	Contains the release notes for this patch kit.
Chapter 2	Summarizes the base operating system patches included in the kit.
Chapter 3	Summarizes the TruCluster software patches included in the kit.

Related Documentation

In addition to this manual, you should be familiar with the concepts and mechanisms described in the following Tru64 UNIX and TruCluster (TCR) documents:

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

Reader’s Comments

HP 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:

  Hewlett-Packard Company
  HCTO Information Development 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.
- The version of TruCluster software that you are using.
- If known, the type of processor that is running the Tru64 UNIX software.

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

1

Release Notes

This chapter provides information that you must be aware of when working with Tru64 UNIX Version 4.0F and TruCluster Software Products Version 1.6 Patch Kit-0008.

1.1 Patch Process Resources

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

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

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

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

  http://h30097.www3.hp.com/docs/patch/index.html

- To visit HP's main support page:

  http://h71025.www7.hp.com/support/home/index.asp

- To visit the Tru64 UNIX homepage:

  http://h30097.www3.hp.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. It is recommended that this kit not be placed in the `/`, `/usr`, or `/var` file systems because this may unduly constrain the available storage space for the patching activity.

- Permanent Storage Space

  Up to ~37 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 ~40 MB of storage space in `/var/adm/patch` may be required for original files if you choose to install and revert all patches. See *Patch Kit Installation Instructions* for more information.

  Up to ~2236 KB of storage space is required in `/var/adm/patch/doc` for patch abstract and README documentation.

  A total of ~176 KB of storage space is needed in `/usr/sbin/dupatch` for the patch management utility.

TruCluster Software Products

- Temporary Storage Space

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

- Permanent Storage Space

  Up to ~37 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 ~40 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 ~2018 KB of storage space is required in /var/adm/patch/doc for patch abstract and README documentation.

  A total of ~176 KB of storage space is needed in /usr/sbin/dupatch for the patch management utility.

1.3 Files Listed as UNKNOWN Origin

If you install the latest patch kit, and run the Baselining feature before you install any aggregate patches, you will get the following files listed as having UNKNOWN origin. This does not represent an error with the operating system or any of the layered products. Ignore this message and proceed with the installation.

```
    * list of changed files with unknown origin:
      ------------------------------------------

  ./usr/.smdb./AFAADVANCED400.scp_extension     OSFBASE440     UNKNOWN
  ./usr/.smdb./AFAADVANCED401.scp_extension     OSFBASE440     UNKNOWN
  ./usr/.smdb./AFAADVANCED402.scp_extension     OSFBASE440     UNKNOWN
  ./usr/.smdb./AFAADVANCED403.scp_extension     OSFBASE440     UNKNOWN
  ./usr/.smdb./AFAADVANCED404.scp_extension     OSFBASE440     UNKNOWN
  ./usr/.smdb./AFAADVANCED425.scp_extension     OSFBASE440     UNKNOWN
  ./usr/.smdb./AFAADVANCED435.scp_extension     OSFBASE440     UNKNOWN
  ./usr/.smdb./AFAADVMAN400.scp_extension       OSFBASE440     UNKNOWN
  ./usr/.smdb./AFAADVMAN401.scp_extension       OSFBASE440     UNKNOWN
  ./usr/.smdb./AFAADVMAN402.scp_extension       OSFBASE440     UNKNOWN
  ./usr/.smdb./AFAADVMAN403.scp_extension       OSFBASE440     UNKNOWN
  ./usr/.smdb./AFAADVMAN404.scp_extension       OSFBASE440     UNKNOWN
  ./usr/.smdb./AFAADVMAN425.scp_extension       OSFBASE440     UNKNOWN
  ./usr/.smdb./AFAADVMAN435.scp_extension       OSFBASE440     UNKNOWN

    * no missing files detected
```

1.4 NHD Installation

If you want to apply NHD3 on V4.0F then it should be done before the Patch Kit-0008 installation. The installation path of V 4.0F to Patch Kit-0008 to NHD3 is not supported in Patch Kit-0008 and may lead to an inconsistent state. The correct installation path is V4.0F to NHD3 to Patch Kit-0008.

1.5 Inclusion of Base Level in tar File Name

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

1.6 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.

1.7 Release Note for DEC 7000 Upgrades to AlphaServer 8400

This release note concerns systems that were upgraded from DEC 7000 to AlphaServer 8400 that have not installed the DWLPA-AA, DWLPB-AA, or the KFTIA. These are the I/O enhancements for the AlphaServer 8400.

Add the following information to the `/sys/conf/SYSTEMNAME` file:

```
bus             tiop0      at tlsb0     vector    tioperror
bus             pci0       at tiop0     slot  0
callout after_c "../bin/mkdata pci"

bus             isp0       at pci0      slot  0 vector    ispintr
controller      scsi0      at isp0      slot  0
```

You must do this on every reconfiguration of the system.

1.8 Release Notes for Tru64 UNIX Patches 476.00 and 351.00

The following release notes provide Visual Threads Upgrade information and updated information for the `quotacheck`(8), `fsck`(8), and `fstab`(4) reference pages.

1.8.1 Visual Threads Upgrade Required

Visual Threads users will need to upgrade to the latest version of Visual Threads for the race detection rules to work. The Visual Threads upgrade is available from **`http://www.tru64unix.compaq.com/visualthreads`** and will be available in the next Developer's Tooklit Supplement.

1.8.2 quotacheck(8), fsck(8), and fstab(4) Reference Pages

quotacheck(8) Reference Page Update

```
SYNOPSIS

  /usr/sbin/quotacheck [-guv] filesystem ...

OLD>  /usr/sbin/quotacheck -a [-guv] [-l number]
NEW>  /usr/sbin/quotacheck -a [-guv] [-l number] [-t [no]type]


FLAGS

OLD>  -a    Checks all file systems identified in the /etc/fstab file
      as read/write with disk quotas.

NEW>  -a    Checks all UFS and AdvFS file systems identified in the
      /etc/fstab file as read/write with userquota and/or
      groupquota options specified, and a pass number of 1 or
      greater.  If the -t option is specified, only the file systems
      of the specified type will be checked.  Alternatively, if
      type is prefixed with 'no', then the valid file systems in
      the /etc/fstab file that do not have that type will be
      checked.


OLD>  -l    number Specifies the number of times to perform disk quota
      checking.

NEW>  -l    number Specifies the maximum number of parallel quotacheck
      processes to run at one time.

NEW>  -t    [no]type
NEW>        Specifies the file system type.  The supported file systems are
      as follows:

      advfs - Advanced File System (AdvFS)

      ufs - UNIX File System (UFS)
```

See fstab(4) for a description of file system types. If the 'no' prefix is used, all of the above file types except the one specified are checked.

Note, the -t flag is only valid when used with the -a flag.

DESCRIPTION

OLD> The quotacheck command examines each specified file system, builds a table of current disk usage, and compares this table against that stored in the disk quota file for the file system. If any inconsistencies are detected, both the quota file and the current system copy of the incorrect quotas are updated. Each file system must be mounted with quotas enabled.

NEW> The quotacheck command examines each specified file system, builds a table of current disk usage, and compares this table against that stored in the disk quota file for the file system. If any inconsistencies are detected, both the quota file and the current system copy of the incorrect quotas are updated.

OLD> The quotacheck command runs parallel passes on file systems using the number specified in the fsck field of the file system's entry in the /etc/fstab file. The quotacheck command only checks file systems with pass number 1 or higher in the fsck field. A file system with no pass number is not checked.

NEW> The quotacheck -a command runs parallel passes on file systems using the number specified in the /etc/fstab pass number field. The quotacheck command only checks file systems with pass number 1 or higher in the fsck field. A file system with no pass number is not checked.

OLD> For both UFS file systems and AdvFS filesets, you should assign the root file system a fsck field value of 1, and a value of 2 or higher to other file systems. See fstab(4) for more information.

NEW> For both UFS file systems and AdvFS filesets, you should assign the root file system a pass number of 1, and a value of 2 or higher to other file systems. See fstab(4) for more information.

OLD> The quotacheck command checks only file systems that have the userquota or groupquota option specified in the /etc/fstab file.

NEW> The quotacheck command checks only file systems that are mounted. UFS file systems must also have userquota and/or groupquota options specified in the /etc/fstab file. The userquota and groupquota options are only needed for AdvFS file systems if quotas are actually going to be enforced or if they are to be selected with the -a option.

fsck(8) Reference Page Update

OLD> When the system boots, the fsck program is automatically run with the -p flag. The program reads the /etc/fstab file to determine which file systems to check. Only partitions that are specified in the fstab file as being mounted “rw” or “ro” and that have a non-zero pass number are checked. File systems that have a pass number 1 (usually only the root file system) are checked one at a time. When pass 1 completes, all the remaining file systems are checked, with one process running per disk drive.

NEW> When the system boots, the fsck program is automatically run with the -p flag. The program reads the /etc/fstab file to determine which file systems to check. Only partitions that are specified in the fstab file as being mounted “rw” or “ro” and that have a non-zero pass number are checked. File systems that have a pass number 1 (usually only the root file system) are checked one at a time. When pass 1 completes, the remaining pass numbers are processed with one parallel fsck process running per disk drive in the same pass.

NEW> The per disk drive logic is based on the /dev/disk/dsk0a syntax where different partition letters are treated as being on the samedisk drive. Partitions layered on top of an LSM device may not follow this naming convention. In this case unique pass numbers in /etc/fstab may be used to sequence fsck checks.

fstab(4) Reference Page Update

userquota [=filename] and groupquota [=filename]

If quotas are to be enforced for users or groups, one or both of the options must be specified. If userquota is specified, user quotas are to be enforced. If groupquota is specified, group:

OLD> quotas are to be enforced.

NEW> quotas are to be enforced (also see quotaon and quotaoff(8)).

OLD> For UFS file systems, the sixth field (fsck) is used by the fsck command to determine the order in which file system checks are done at reboot time. For the root file system, specify 1 in the fsck field. For other UFS file systems, specify 2 or higher in the fsck field. Each UFS file system should have a unique fsck value.

NEW> For UFS file systems, the sixth field (pass number) is used by the fsck and quotacheck commands to determine the order in which file system checks are done at reboot time. For the root file system, specify 1 in the fsck field. For other UFS file systems specify 2 or higher in the pass number field.

OLD> For AdvFS filesets, the sixth field is a pass number field that allows the quotacheck command to perform all of the consistency checks needed for the fileset. For the root file system, specify 1 in the fsck field. Each AdvFS fileset in an AdvFS file domain should have a unique fsck value, which should be 2 or higher.

NEW> For AdvFS filesets, the sixth field is a pass number field that allows the quotacheck command to perform all of the consistency checks needed for the fileset. For the root file system, specify 1 in the fsck field. For other AdvFS file systems specify 2 or higher in the pass number field.

OLD> File systems that are on the same disk are checked sequentially, but file systems on different disks are checked at the same time to utilize parallelism available in the hardware. If the sixth field is not present or zero, a value of 0 is returned and the fsck command assumes that the file system does not need to be checked.

NEW> File systems that are on the same disk or domain are checked sequentially, but file systems on different disks or domains but with the same or greater than 1 pass number are checked at the same time to utilize parallelism available in the hardware. When all the file systems in a pass have completed their checks, then the file systems with the numerically next higher pass number will be processed.

NEW> The UFS per disk drive logic is based on the /dev/disk/dsk0a syntax where different partition letters are treated as being on the same disk drive. Partitions layered on top of an LSM device may not follow this naming convention. In this case unique pass numbers may be used to sequence fsck and quotacheck processing. If the sixth

field is not present or zero, a value of 0 is returned
and the fsck command assumes that the file system does
not need to be checked.

1.9 Release Note for Tru64 UNIX Patch 315.00

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

If the system configurable parameter `lsm:lsm_V_ROUND_enhanced` is `set` (value = 1) the enhanced read round robin policy is activated. This new policy stores the last block accessed by the previous I/O request. When returning for another block in round robin (`V_ROUND`) mode, that value is compared to the current read. If it is within a predefined, user-configurable value (`lsm:lsm_V_ROUND_enhance_proximity`), then the same plex is used. Otherwise the next plex is used as for a normal round robin behavior.

The two new additional tunable parameters are `lsm_V_ROUND_enhanced` set to 1 by default (`V_ROUND` read is activated) and `lsm_V_ROUND_enhance_proximity` is set to 512 by default.

Append any tuning changes to`/etc/sysconfigtab`. See the TUNING notes below for a description of the new `lsm_V_ROUND_enhanced` and `lsm_V_ROUND_enhance_proximity` tunables. These tunables are configured in the `lsm` stanza. For example:

```
lsm:

lsm_V_ROUND_enhanced = 1

lsm_V_ROUND_enhance_proximity = 1024
```

Note

If you already have an `lsm` stanza in your `sysconfigtab` file, add the two `lsm_V_ROUND` entries.

TUNING

The purpose of this patch is to increase performance with sequential reads. This patch introduces a new enhanced round robin mode where the last block read is now compared to the next block to read and a check is added to see if last block number-next block number is less than or equal to `lsm_V_ROUND_enhance_proximity`. If it is, read from the same plex. This is to attempt to hit the disk cache, and so increase performance.

The relevant tunable variables are as follows:

`lsm_V_ROUND_enhanced`

This variable activates the new enhanced round robin read policy if it is set to TRUE (1). Otherwise the policy is deactivated.

DEFAULT = 1

`lsm_V_ROUND_proxmity`

This variable provides the proximity in which the last read and new read most lie in an attempt to read data from the disk’s cache by reading from the same plex. The variable can be adjusted from 0 to 4096.

DEFAULT = 512

1.10 Release Note for Tru64 UNIX Patch 351.00

For more information about the functionality provided and special installation instructions related to this patch, please refer to the online README file located at:

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

From this directory, click on the following link:

duv40fwlseco2.README

Note

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

1.11 Release Note for Tru64 UNIX Patch 592.00

This patch contains a solution for the following issue:

HP has advised owners of DS10, DS10L, ES40 AlphaServers, and XP900 AlphaStations that HP 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 HP has observed the anomaly only in laboratory tests designed to create atypical system stresses, including almost constant use of the floppy disk drive, HP has informed owners of the remote possibility that the anomaly could occur so that they may take precautions to prevent it.

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

The solution to this issue is also available as an individual, manually installed patch kit named `floppy_CSP_v40g.tar.gz`, available from:

http://ftp1.support.compaq.com/public/unix/v4.0g

1.12 Release Note for Tru64 UNIX Patches 1197.00 and 1199.00

This patch delivers version V1.0-032 of the libots3 library. Version 2.0 of the 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_V4.0F / Software Development Environment Patches:

Patch 00XXX.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.so:

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

1.13 Release Note for Tru64 UNIX Patch 1331.00

This patch provides the X server support for the new 3DLabs Oxygen VX1 PCI graphics card. In order to obtain full support for this graphic card, you must also select Patch 1493.00, 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`

1.14 Release Note for Tru64 UNIX Patch 1414.00

This release note contains the new `fixfdmn`(8) reference page.

NAME

fixfdmn - Checks and repairs corrupted AdvFS domains

SYNOPSIS

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

/sbin/advfs/fixfdmn -u directory domain

OPTIONS

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

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

-d directory

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

-m type[,type...]

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

sync

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

log Resets the transaction log so it is not processed.

sbm Synchronizes the sbm to the information in the bmt.

bmt Corrects the bmt.

frag

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

quota
Checks and corrects sizes of quota files.

files
Verifies that directory metadata is correct.

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

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

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

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

0 = Only error messages

1 = (Default) Progress, errors and summary messages

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

OPERANDS

domain
The name of a corrupted domain to repair.

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

DESCRIPTION

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

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

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

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

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

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

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

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

NOTES

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

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

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

RESTRICTIONS

You must be root to run fixfdmn.

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

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

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

EXIT STATUS

0 (Zero)
Success.

1 Corrupt
Unable to repair all found corruptions

2 Failure
Program or system error

FILES

/etc/fdmns
Contains AdvFS domain directories and locks.

SEE ALSO

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

1.15 Release Note for Tru64 UNIX Patch 1320.00 and 1323.00

This patch updates the BIND version from V4 to V8.3.4 in order to provide a more secure version of BIND. In particular, it addresses the vulnerability described in SSRT2400, for which HP had previously published a workaround. The BINDv8 shipped here does not include the `dnskeygen` utility and thus cannot generate its own transaction keys. However, it can be configured to participate as a slave in a zone transfer that uses transaction keys.

BINDv8 uses a configuration file with a different name and format than that of BINDv4. The `/usr/sbin/named-bootconf` utility will convert the BINDv4 `named.boot` file to a BINDv8 `named.conf` file. After installing this patch, you must use the `/usr/sbin/named-bootconf` utility to convert your configuration file. Connect to the directory that contains the `named.boot` file, normally `/etc/namedb`, then run the conversion utility as shown:

```
/usr/sbin/named-bootconf < /etc/namedb/named.boot > /etc/namedb/named.conf
```

Then use /usr/sbin/rcmgr to insert the correct configuration filename in the BIND starting arguments, as shown:

```
/usr/sbin/rcmgr set BIND_SERVERARGS -c /etc/namedb/named.conf
```

At this point you may now stop the old server (if you have not already), and start the new named. Use these commands:

```
/sbin/init.d/named stop
/sbin/init.d/named start
```

If at any time you rerun bindsetup or bindconfig, make sure to run these /usr/sbin/named-bootconf and /usr/sbin/rcmgr commands again afterward.

Updated versions of the BIND Configuration Guide and the *Network Administration: Services* guide can be found on the Tru64 UNIX documentation website, **http://h30097.www3.hp.com/docs/pub_page/doc_list.html**.

Updated reference pages ship with this patch kit.

1.16 Release Note for Tru64 UNIX Patch 1421.00

A new Russian keyboard comes with 5 extra keycaps. To enable any of the extra keycaps, you will need to modify the /usr/lib/X11/xkb/symbols/digital_russian file. For example,

```
//    KEY <AD09> can be replaced by an extra keycap.
//    If you replace it with the extra keycap, please uncomment
//    the following definition and comment out the original one.
//
//    key <AD09> {
//      symbols[Group1]=3D [              o,              O ],
//      symbols[Group2]=3D [     Ukrainian_i,     Ukrainian_I ]
//    };
    key <AD09> {
        symbols[Group1]=3D [              o,              O ],
        symbols[Group2]=3D [  Cyrillic_shcha,  Cyrillic_SHCHA ]
    };
```

1.17 Release Notes for Tru64 UNIX Patch 1493.00

This section contains release notes for Patch 1493.00.

1.17.1 Update to the getsockopt(2), accept(2), getsockname(2), and getpeername(2) References Pages

This patch updates the getsockopt(2), accept(2), getsockname(2), and getpeername(2) references pages with the following change in the ERRORS section:

[EINVAL]

> The option_value or option_len parameter is invalid; or the socket is shut down.

These changes were not made to the on line reference pages.

1.17.2 New Security Feature, No Execute Heap/Data

Caution

Read this release note completely and execute the /usr/sbin/javaexecutedata script before enabling this feature.

This patch kit introduces a new security feature called no execute heap/data, similar in concept to Tru64 UNIX's executable stack protection. When enabled, the feature prevents the execution of instructions that reside in heap or other data areas of process memory, providing additional protection against buffer overflow exploits.

In a buffer overflow exploit, an attacker feeds a privileged program an unexpectedly large volume of carefully constructed data through inputs such as command-line arguments and environment variables. If the program is not coded defensively, the attacker can overwrite areas of memory adjacent to the buffer. Depending upon the location of the buffer (stack, heap, data area), the attacker can deceive these programs into executing malicious code that takes advantage of the program's privileges, or alter a security-sensitive program variable to redirect program flow. Such an attack can be used to gain root access to the system.

Enabling the `executable_data` tunable changes a potential system compromise into, at worst, a denial of service attack. A vulnerable program may still contain a buffer overflow, but an exploit that writes an instruction stream into the buffer and attempts to transfer control to those instructions will fail, because memory protection will prohibit instruction execution from that area of memory.

The new feature is implemented as a dynamic `sysconfig` tunable, `executable_data` in the `proc` subsystem. The supported settings allow a system administrator to cause requests from privileged processes for writable and executable memory to fail, or to be treated as a request for writable memory, and to optionally generate a message when such a request occurs. Many applications unnecessarily request write-execute memory directly, or because of the default of some underlying function acting on their behalf, but never execute from the memory. By substituting writable memory for the requested write-execute memory, the `executable_data` tunable allows such applications to benefit from the additional protection without requiring application modification.

Five settings are supported for the `executable_data` tunable:

0 Disabled, the default setting. All processes may allocate writable and executable memory.

5 The recommended setting. When a process executing as root or a process running a `setuid` application requests writable, executable memory, the request succeeds but the process receives only writable memory. No message is generated.

21 When a process executing as root or a process running a `setuid` application requests writable, executable memory, the request fails with an EACCES status and no message is generated.

37 When a process executing as root or a process running a `setuid` application requests writable, executable memory, the request succeeds, the process receives only writable memory, and a message is generated.

53 When a process executing as root or a process running a `setuid` application requests writable, executable memory, the request fails with an EACCES status and a message is generated.

No other settings are supported. Attempting to use unsupported settings can cause unexpected and undesirable application behavior.

Note

> Before changing executable_data from the default value of 0, you must run the /usr/sbin/javaexecutedata script. Otherwise, privileged java applications will fail in unpredictable ways. The Java language does not compile programs, but instead interprets them as they run. Unless marked as exempt, privileged applications written in Java will receive an error when they attempt to execute instructions residing in the unexecutable memory. The manner in which they handle the error is application-specific and thus unpredictable. If you plan to enable the executable_data tunable, you MUST use the /usr/sbin/javaexecutedata script.

Privileged Pascal programs that use non-local gotos may also fail. Such programs should also be marked as exempt, using the new chatr utility as follows:

```
$chatr +ed enable priv_pascal_executable
  current values:
     64-bit COFF executable
     execute from data: disabled
  new values:
     64-bit COFF executable
     execute from data: enabled
```

This example demonstrates the failing behavior to expect for privileged processes if you set execute_data to 53 but do not run the /usr/sbin/javaexecutedata script. Other Java applications run with privilege may exhibit different (but still failing) behavior.

```
# java -classic -jar SwingSet2.jar
Process 1185 Invalid write/execute mmap call denied.
Process 1185 Invalid write/execute mmap call denied.
Process 1185 Invalid write/execute mmap call denied.
(...)
Process 1185 Invalid write/execute mmap call denied.
Process 1185 Invalid write/execute mmap call denied.
**Out of memory, exiting**
```

This example demonstrates the failing behavior to expect for privileged processes if you set execute_data to 37 but do not run the /usr/sbin/javaexecutedata script. Other Java applications run with privilege may exhibit different (but still failing) behavior.

```
# java -classic -jar SwingSet2.jar
Process 1185 Invalid write/execute mmap call modified.
Process 1185 Invalid write/execute mmap call modified.
 (...)
Process 1185 Invalid write/execute mmap call modified.
Process 1185 Invalid write/execute mmap call modified.
Process 1185 Invalid write/execute mmap call modified.
SIGSEGV   11*  segmentation violation
(...)
Abort (core dumped)
```

1.17.3 Security Vulnerability

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 access. HP has corrected this potential vulnerability.

In addition the following changes were made:

- shell inline input files are more secure

- sh noclobber and new constructs added

Updated sh, csh and ksh

The updated shells in this kit all implement the following changes when processing shell inline input files:

- File permissions allow only read and write for owner
- If excessive inline input file name collisions occur the the following error message will be returned:

  ```
  Unable to create temporary file
  ```

sh noclobber option and >| , >>| constructs added

A `noclobber` option similar to that already available with `csh` and `ksh` has been added to the Bourne shell.

When the `noclobber` option is used (`set -C`), the shell behavior for the redirection operators > and >> changes as follows:

- For > with `noclobber` set, `sh` will return an error rather than overwrite an existing file. If the specified file name is actually a symlink, the presence of the symlink satisfies the criteria `file exists` whether or not the symlink target exists, and `sh` returns an error. The >`|` construct will suppress these checks and create the file.
- For >> with `noclobber` set, output is appended to the tail of an existing file. If the file name is actually a symlink whose target does not exist, `sh` returns an error rather than create the file. The >>`|` construct will suppress these checks and create the file.

ksh noclobber behavior clarified

For > with `noclobber` set, `ksh` returns an error rather than overwrite an existing file. If the file name is actually a symlink, the presence of the symlink satisfies the criteria `file exists` whether or not the symlink target exists, and `ksh` returns an error. The >`|` construct will suppress these checks and create the file.

For >> with `noclobber` set, output is appended to the tail of an existing file. If the file name is actually a symlink to a non-existent file, `ksh` returns an error.

csh noclobber behavior clarified

For > with `noclobber` set, `csh` returns an error rather than overwrite an existing file. If the file name is actually a symlink, the presence of the symlink satisfies the criteria `file exists` whether or not the symlink target exists, and `csh` returns an error. The >! construct will suppress these checks and create the file.

1.17.4 New sys_check Reference Page

NAME

sys_check, runsyscheck - Generates system configuration information and analysis

SYNOPSIS

/usr/sbin/sys_check [options...]

OPTIONS

-all

Lists all subsystems, including security information and setld inventory verification. This option may take a long time to complete.

-debug
Outputs debugging information to stderr (standard error output).

-escalate [xx]
Creates escalation files for reporting problems to your technical support representative. This option produces one file, TMPDIR/escalate.tar unless there are crash dump files; if so, it also creates two other files: TMPDIR/escalate_vmunix.xx.gz and TMPDIR/escalate_vmcore.xx.gz. If you use the -escalate option, sys_check runs with the -noquick option and collects the output in the escalate.tar file. Optionally, you can specify a number (xx) with the -escalate option to define a crash number.

See also the ENVIRONMENT VARIABLES section for information on how you can set the value of TMPDIR.

-evm
Generates Event Manager (EVM) warnings. When EVM is configured, warnings are posted as EVM events identified by the string sys.unix.sys_check.warning. Six levels of priority ranging from 0-500 are used, as follows:

+ 0 - Information only.

+ 100 - Note

+ 200 - Tuning Note

+ 300 - Tuning Suggestion

+ 400 - Operational

+ 500 - Warning

-frame
Produces frame HTML output, which consists of three files: sys_checkfr.html, sys_checktoc.html, and sys_check.html (unless you specify a different file name with the -name option). This option cannot be used with the -nohtml option. The following options are available for use with the -frame option:

-name name
Specifies the name to use for the frame files output. The default name is sys_check.

-dir name
Sets the directory for the frames output. Used only with the -frame option. The default is the current directory (.).

-help or (-h)
Outputs help information.

-nohtml
Produces text output, consisting of one text file, instead of the default HTML output. This option cannot be used with the -frame option.

-noquick
Outputs configuration data and the setld scan. Excludes security information.

-perf
Outputs only performance data and excludes configuration data. This option takes less time to run than others.

-v Displays the sys_check version number.

-warn
Executes only the warning pass. This option takes less time to run than other options.

-nowarn

Executes only the data gathering pass.

DESCRIPTION

The sys_check utility is a system census and configuration verification tool that is also used to aid in diagnosing system errors and problems. Use sys_check to create an HTML report of your system's configuration (software and hardware). The size of the HTML output that is produced by the sys_check utility is usually between .5 MB and 3 MB.

The sys_check utility also performs an analysis of operating system parameters and attributes such as those that tune the performance of the system. The report generated by sys_check provides warnings if it detects problems with any current settings. Note that while sys_check can generate hundreds of useful warnings, it is not a complete and definitive check of the health of your system. The sys_check utility should be used in conjunction with event management and system monitoring tools to provide a complete overview and control of system status. Refer to the EVM(5) reference page for information on event management. Refer to the System Administration guide for information on monitoring your system.

When used as a component of fault diagnosis, sys_check can reduce system down time by as much as 50% by providing fast access to critical system data. It is recommended that you run a full check at least once a week to maintain the currency of system data. However, note that some options will take a long time to run and can have an impact on system performance. You should therefore choose your options carefully and run them during off-peak hours. As a minimum, perform at least one full run (all data and warnings) as a post-configuration task in order to identify configuration problems and establish a configuration baseline. The following table provides guidelines for balancing data needs with performance impact.

Option	Run time	Performance impact	Recommended At
-warn, -perf	Short.	Minimal.	Regular updates, at least weekly
null - no options selected.	Medium, perhaps 15 to 45 minutes depending on processor.	Some likely at peak system use.	Run at least once post-installation and update after major configuration changes. Update your initial baseline and check warnings regularly.
-noquick, -all, -escalate.	Long, perhaps 45 minutes on fast, large systems to hours on low-end systems.	Very likely at peak use.	Use only when troubleshooting a system problem or escalating a problem to your technical support representative.

You can run some sys_check options from the SysMan Menu or the /usr/sbin/sysman -cli command-line interface. Choose one of the following options from the Menu:

>- Support and Services
  | Create escalation report [escalation]
  | Create configuration report [config_report]

Alternatively, use the config_report and escalation accelerators from the command line. Note that the escalation option should only be used in conjunction with a technical support request.

The runsyscheck script will run sys_check as a cron task automatically if you do not disable the crontab entry in /var/spool/cron/crontabs/root.

Check for the presence of an automatically generated log file before you create a new log, as it may save time.

When you run the sys_check utility without command options, it gathers configuration data excluding the setld scan and the security information and displays the configuration and performance data by default. It is recommended that you do this at least once soon after initial system configuration to create a baseline of system configuration, and to consider performing any tuning recommendations.

On the first run, the sys_check utility creates a directory named /var/recovery/sys_check. On subsequent runs, sys_check creates additional directories with a sequential numbering scheme:

+ The previous sys_check directory is renamed to /var/recovery/sys_check.0 while the most recent data (that is, from the current run) is always maintained in /var/recovery/sys_check.

+ Previous sys_check directories are renamed with an incrementing extension; /var/recovery/sys_check.0 becomes /var/recovery/sys_check.1, and so on, up to /var/recovery/sys_check.5.

There is a maximum of seven directories. This feature ensures that you always have up to seven sets of data automatically. Note that if you only perform a full run once, you may want to save the contents of that directory to a different location.

Depending on what options you choose, the /var/recovery/sys_check.* directories will contain the following data:

+ Catastrophic recovery data, such as an etcfiles directory, containing copies of important system files. In this directory, you will find copies of files such as /etc/group, /etc/passwd, and /etc/fstab.

+ Formatted stanza files and shell scripts and that you can optionally use to implement any configuration and tuning recommendations generated by asys_check run. You use the sysconfigdb command or run the shell scripts to implement the stanza files. See the sysconfigdb(8) reference page for more information.

NOTES

You must be root to invoke the sys_check utility from the command line; you must be root or have the appropriate privileges through Division of Privileges (DoP) to run Create Configuration Report and Create Escalation Report from the SysMan Menu. The sys_check utility does not change any system files.

The sys_check utility is updated regularly. You can obtain the latest version of the sys_check utility from either of two sources:

+ The most up-to-date version of the sys_check kit is located on the sys_check tool web site, http://www.tru64unix.compaq.com/sys_check/sys_check.html

+ You can also obtain sys_check from the patch kit, see http://www.support.compaq.com/patches/.

You should run only one instance of sys_check at a time. The sys_check utility prevents the running of multiple instances of itself, provided that the value of the TMPDIR environment variable is /var/tmp, /usr/tmp, /tmp, or a common user-defined directory. This avoids possible collisions when an administrator attempts to run sys_check while another administrator is already running it. However, no guarantees can be made for the case when two administrators set their TMPDIR environment variables to two different user-defined directories (this presumes that one administrator does not choose /var/tmp, /usr/tmp, or /tmp).

The sys_check utility does not perform a total system analysis, but it does check for the most common system configuration and operational problems on production systems.

Although the sys_check utility gathers firmware and hardware device revision information, it does not validate this data. This must be done by qualified support personnel.

The sys_check utility uses other system tools to gather an analyze data. At present, sys_check prefers to use DECevent and you should install and configure DECevent for best results.

If DECevent is not present, the sys_check utility issues a warning message as a priority 500 EVM event and attempts to use uerf instead. In future releases, Compaq Analyze will also be supported on certain processors.

Note that there are restrictions on using uerf, DECevent and Compaq Analyze that apply to:

+ The version of UNIX that you are currently using.

+ The installed version of sys_check.

+ The type of processor.

EXIT STATUS

The following exit values are returned:

0   Successful completion.

>0 An error occurred.

LIMITATIONS

DECevent or Compaq Analyze may not be able to read the binary error log file if old versions of DECevent are being used or if the binary.errlog file is corrupted. If this problem occurs, install a recent version of DECevent and, if corrupted, recreate the binary.errlog file.

HSZ controller-specific limitations include the following:

HSZ40 and HSZ50 controllers:
The sys_check utility uses a free LUN on each target in order to communicate with HSZ40 and HSZ50 controllers. To avoid data gathering irregularities, always leave LUN 7 free on each HSZ SCSI target for HSZ40 and HSZ50 controllers.

HSZ70, HSZ80 and HSG80 controllers:
The sys_check utility uses a CCL port in order to communicate with HSZ70 controllers. If a CCL port is not available, sys_check will use an active LUN. To avoid data gathering irregularities, enable the CCL port for each HSZ70 controller.

HSV controller-specific limitations include the following:

The sys_check utility uses the SANscript utility (sssu) to collect data from the Enterprise controller. This utility is included with the Enterprise Package Kit. Please install this utility in /usr/lbin and ensure that it has execute permissions.

The sys_check utility cannot dynamically determine the SAN appliance or appliances used to manage your Enterprise storage.To do so, create the file /etc/enterprise.txt with the element name, the user name, and the password (separated by colons) of the SAN appliance as shown below; these values may contain embedded spaces. Set the permissions of this file to 600.

```
    element:user:password
    element 1:user 1:password
```

The sys_check utility attempts to check the NetWorker backup schedule against the /etc/fstab file. For some older versions of Networker, the nsradmin command contains a bug that prevents sys_check from correctly checking the schedule. In addition, the sys_check utility will not correctly validate the NetWorker backup schedule for TruCluster services.

EXAMPLES

1. The following command creates escalation files that are used to report problems to your technical support organization:
   ```
   # sys_check -escalate
   ```

2. The following command outputs configuration and performance information, excluding security information and the setld inventory, and provides an analysis of common system configuration and operational problems:
   ```
   # sys_check > file.html
   ```

3. The following command outputs all information, including configuration, performance, and security information and a setld inventory of the system:
   ```
   # sys_check -all > file.html
   ```

4. The following command outputs only performance information:
   ```
   # sys_check -perf > file.html
   ```

5. The following command provides HTML output with frames, including configuration and performance information and the setld inventory of the system:
   ```
   # sys_check -frame -noquick
   ```

6. The following command starts the SysMan Menu config_report task from the command line:
   ```
   # /usr/sbin/sysman config_report
   ```

   Entering this command invokes the SysMan Menu, which prompts you to supply the following optional information:

   + Save to (HTML) - A location to which the HTML report should be saved, which is /var/adm/hostname_date.html by default.

   + Export to Web (Default) - Export the HTML report to Insight Manager. Refer to the System Administration for information on Insight Manager.

   + Advanced options - This option displays another screen in which you can choose a limited number of run time options. The options are equivalent to certain command line options listed in the OPTIONS section.

     In this screen, you can also specify an alternate temporary directory other than the default of /var/tmp.

   + Log file - The location of the log file, which is /var/adm/hostname_date.log by default.

7. The following is an example of a stanza file advfs.stanza in /var/recovery/sys_check.*:
   ```
   advfs:
   AdvfsCacheMaxPercent=8
   ```

8. The following is an example of a shell script apply.kshin /var/recovery/sys_check.*:
   ```
   cd /var/cluster/members/member/recovery/sys_check/
   llist="advfs.stanza
   vfs.stanza "
   for stf in $llist; do
   print " $stf "
           stanza=‘print $stf | awk -F . ’{print $1 }”‘
   print "/sbin/sysconfigdb -m -f $stf $stanza"
           /sbin/sysconfigdb -m -f $stf $stanza
   done
   print "The system may need to be rebooted for these
   changes to take effect"
   ```

ENVIRONMENT VARIABLES

The following environment variables affect the execution of the sys_check utility. Normally, you only change these variables under the direction of your technical support representative, as part of a fault diagnosis procedure.

TMPDIR
Specifies a default parent directory for the sys_check working subdirectory, whose name is randomly created; this working subdirectory is removed when sys_check exits. The default value for TMPDIR is /var/tmp.

LOGLINES
Specifies the number of lines of log file text that sys_check includes in the HTML output. The default is 500 lines.

BIGNUMFILE
Specifies the number of files in a directory, above which a directory is considered excessively large. The default is 15 files.

BIGFILE
Specifies the file size, above which a file is considered excessively large. The default is 3072 KB.

VARSIZE
Specifies the minimum amount of free space that sys_check requires in the TMPDIR directory. The default is 15 MB and should not be reduced. The sys_check utility will not run if there is insufficient disk space.

RECOVERY_DIR
Specifies the location for the sys_check recovery data. The default is /var/recovery. The sys_check utility automatically cleans up data from previous command runs. The typical size of the output generated by each sys_check utility run is 400 KB. This data may be useful in recovering from a catastrophic system failure.

ADHOC_DIR
Specifies the location at which sys_check expects to find the text files to include in the HTML output. The default is the /var/adhoc directory.

TOOLS_DIR
Specifies the location at which sys_check expects to find the binaries for the tools that it calls. The default is /usr/lbin.

FILES

/usr/sbin/sys_check
Specifies the command path.

Note

This file may be a symbolic link.

/usr/lbin/*
Various utilities in this directory are used by sys_check.

Note

These files may be symbolic links.

The sys_check utility reads many system files.

SEE ALSO

Commands: dop(8), sysconfigdb(8), sysman_cli(8), sysman_menu(8)

Miscellaneous: EVM(5), insight_manager(5)

Books: System Administration, System Tuning

1.17.5 tar/pax/cpio Behavior

This is regarding the behavior of `tar/pax/cpio`, when a slash (/) is specified at the end of an argument. While extracting or listing an archive, if a slash (/) is present at the end of an argument (for example, `tar xvf foo.tar dir1/` or `tar tvf foo.tar dir1/`), then it only acts upon that particular directory and not the contents in the directory. If multiple slashes are used while creating an archive (for example, `tar cvf foo.tar dir1/////////`), previously all these slashes were put in the archive header. Now it will put only one slash for any directory entry in the header. If a single slash is specified while creating the archive, it still picks up all the contents as usual.

The `pax` and `cpio` commands behave in a similar way.

1.17.6 Changes to rexecd Reference Page

This patch contains 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.

1.17.7 mountd Reference Page Update

The following is an update for the `mountd` reference page.

SYNOPSIS
mountd [-d] [-i] [-n] [-s] [-r] [-R] [exportsfile]

FLAGS
...
-r Have mountd listen for requests on a reserved port. This is the default behavior.

-R mountd may listen on an unreserved port.

1.17.8 UFS Delayed Metadata mount Option

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

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

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

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

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

To enable the `delayed` option, run:

```
mount -o delayed
```

or

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

1.17.9 3DLabs Oxygen VX1 Graphics Card

This patch provides the driver support for the 3DLabs Oxygen VX1 graphics card. In order to obtain full support for this graphics card, you must also select Patch 1331.00, 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 reconfigure and rebuild the kernel, 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/update
   ```

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 3DLabs Oxygen VX1 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 3DLabs Oxygen VX1 graphics card as described you will need to rebuild the kernel again to restore generic VGA graphics support. To do this, follow the steps given previously. The `doconfig` utitlity running on the original, unpatched `genvmunix` will not recognize the 3DLabs Oxygen VX1 graphics card and will include generic VGA graphics support in the resulting kernel.

1.17.10 PCI To Ethernet/Graphics Combo Adapter (3X-DEPVD-AA)

This patch provides the driver support for the PCI To Ethernet/Graphics Combo Adapter (3X-DEPVD-AA) (also known as the ITI6021E Fast Ethernet NIC 3D Video Combination Adapter, InterServer Combo, or JIB). To obtain full support for the PCI To Ethernet/Graphics Combo Adapter (3X-DEPVD-AA), you must also select Patch 1326.00, which is the X server portion of the patch.

1.17.11 DEGPA-TA Gigabit Ethernet Device

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

To do this, follow these steps:

1. Shut down the system:

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

2. Boot genvmunix to single-user mode:

   ```
   >>> boot -fi genvmunix -fl s
   ```

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

   ```
   # /sbin/bcheckrc
   # /sbin/update
   # /sbin/swapon -a
   ```

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

   ```
   # /usr/sbin/doconfig
   ```

   Note

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

5. Save the old `/vmunix` file and move the new kernel to `/vmunix`.
6. Shut down the system:

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

7. Boot the new kernel:

   ```
   >>> boot
   ```

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

1.17.12 Intelligent I/O Disks with mnemonic ri

If Patch 1493.00 is installed on a system with Intelligent I/O (I2O) disks that use the device identifier, `mnemonic ri`, Patch 1386.00 should also be installed if the user uses the `diskconfig` utility. Without Patch 1386.00, the `diskconfig` utility will not recognize or configure the Intelligent I/O (I2O) disks.

1.17.13 Virtual Memory Problem

Installing Patch 1493.00 on a system running Tru64 UNIX Versions 4.0D through 4.0F may cause the system to crash if you run an application that maps a large number of file system objects into virtual memory using the mmap(2) function call. This problem may occur with large threaded applications, such as the Netscape Enterprise Web Server, which use this technique to improve performance and scalability.

To avoid this problem, disable the kernel's virtual memory (vm:) subsystem attribute vm-map-index-enable after installing the patch and before rebooting the system. The attribute is disabled when its value is set to zero at boot time.

Enter the following commands at the shell prompt (when logged in as root) to add or modify the vm-map-index-enable attribute entry in the /etc/sysconfigtab file:

```
$ su root
$ cat << _EOF_ > /tmp/vm.stanza
> vm:
> vm-map-index-enabled=0
> _EOF_
$ sysconfigdb -m -f /tmp/vm.stanza vm
$rm -f /tmp/vm.stanza
$ reboot
```

See the sysconfigdb(8) reference page for additional information.

This problem will be fixed in the next release of the patch kits.

1.17.14 PCI To Ethernet/Graphics Combo Adapter

This patch provides support for the PCI To Ethernet/Graphics Combo Adapter (3X-DEPVD-AA). If you have a system with this adapter, 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 PCI To Ethernet/Graphics Combo Adapter.

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 PCI To Ethernet/Graphics Combo Adapter as previously described, you will need to rebuild the kernel again to restore generic VGA graphics support. To do this, follow the steps previously given.

If doconfig is running on the original kernel, the unpatched genvmunix will not recognize the PCI To Ethernet/Graphics Combo Adapter and will include generic VGA graphics support in the resulting kernel.

1.17.15 Pleiades II Switches

This patch fixes a problem with the Pleiades II switches, where the switch ports would consume target IDs on the adapter's SCSI bus.

To determine if target IDs are being consumed by the switch, look at the contents of the /etc/emx.info file. If a FC Port Name exists that does not start with 0x0050 (a HSG80) or a 0x0010 (a KGPSA), it is most likely a switch entry consuming the target ID (or an unsupported FC device exists on the fabric).

To remove the switch entry from the emx target ID mappings, in addition to installing this patch, the /sys/data/emx_data.c file must be modified to contain the switch entry to be deleted (by setting the target ID to -1). See the reference pages for emx and emx_data.c for instructions on modifying the emx_data.c file. After the emx_data.c file has been modified, the kernel must be regenerated and the resulting kernel booted.

1.17.16 I/O Throttling/Smooth Sync

Note

Smooth Sync is for UNIX File System (UFS) only.

Note

To activate I/O Throttling/Smooth Sync, you must install Patch 299.00.

The new mount options are smsync2 and throttle. The smsync2 option enables an alternate smsync policy in which dirty pages do not get flushed until they have been dirty and idle for the smoothsync age period (the default 30 is seconds). The default policy is to flush dirty pages after being dirty for the smoothsync age period, regardless of continued modifications to the page. Note that mmaped pages always use this default policy, regardless of the smsync2 setting.

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

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

to:

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

Note

> If you choose not to use smsync2 (which does not affect mmap buffers), remove the smsync2 option from the previous string.

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

```
vfs:

io-throttle-shift = 1

io-throttle-maxmzthruput = 1
```

When removing this patch, follow these steps:

1. Remove the lines added in the previous example to /etc/inittab.
2. Remove any additions to /etc/fstab you may have made (see previous instructions).

Failure to remove /etc/inittab and /etc/fstab modifications may result in unknown attribute messages, particularly upon system reboot.

TUNING

The purpose of this patch is to minimize system stalls resulting from a heavy system I/O load. This patch introduces a smoothsync approach to writing delayed I/O requests and introduces I/O throttling.

Using smoothsync allows each dirty page to age for a specified time period before getting pushed to disk. This allows more opportunity for frequently modified pages to be found in the cache, which decreases the net I/O load. Also, as pages are enqueued to a device after having aged sufficiently, as opposed to getting flushed by the update daemon, spikes are minimized in which large numbers of dirty pages are locked on the device queue.

I/O throttling further addresses the concern of locking dirty pages on the device queue. It enforces a limit on the number of delayed I/O requests allowed to be on the device queue at any point in time. This allows the system to be more responsive to any synchronous requests added to the device queue, such as a read or the loading of a new program into memory. This may decrease the duration of process stalls for specific dirty buffers, as pages remain available until placed on the device queue.

The relevant tunable variables are:

`smoothsync-age`

This variable can be adjusted from 0 (off) up to 300. This is the number of seconds a page ages before becoming eligible for being flushed to disk via the smoothsync mechanism. A value of 30 corresponds to the "guarantee" provided by the traditional UNIX update mechanism. Increasing this value increases the exposure of lost data should the system crash, but can decrease net I/O load (to improve performance) by allowing the dirty data to remain in cache longer. In some environments, any data that is not up to date is useless; these are prime candidates for an increased smoothsync-age value. The default value of smoothsync-age is 30.

`io-throttle-shift`

The greater the number of requests on an I/O device queue, the longer the time required to process those requests and make those pages and device available. The number of concurrent delayed I/O requests on an I/O device queue can be throttled by setting the io-throttle-shift tunable. The throttle value is based on this tunable and the calculated I/O completion rate. The throttle value is proportional to the time required to process the I/O device queue. The correspondences between io-throttle-shift values and the time to process the device queue are:

io-throttle-shift	time to process device queue (sec)
-2	0.25
-1	0.5
0	1
1	2
2	4

For example, an io-throttle-shift value of 0 corresponds to accommodating 1 second of I/O requests. The valid range for this tunable is [-4..4] (not all values are shown in the previous table; you can extrapolate). The default value of io-throttle-shift is 1. Environments particularly sensitive to delays in accessing the I/O device might consider reducing the io-throttle-shift value.

io-maxmzthruput

This is a toggle that trades off maximizing I/O throughput against maximizing the availability of dirty pages. Maximizing I/O throughput works more aggressively to keep the device busy, but within the constraints of the throttle. Maximizing the availability of dirty pages is more aggressive at decreasing stall time experienced when waiting for dirty pages.

The environment in which you might consider setting io-maxmzthruput off (0) is one in which I/O is confined to a small number of I/O–intensive applications, such that access to a specific set of pages becomes more important for overall performance than does keeping the I/O device busy. The default value of io-maxmzthruput is 1. Environments particularly sensitive to delays in accessing sets of frequently used dirty pages might consider setting io-maxmzthruput to 0.

1.17.17 Granularity Hint Regions Restriction Removal

This patch removes a Granularity Hint Regions (also called GH chunks) restriction which may be encountered on AlphaServerTM™ DS20 and ES40 systems running the Tru64 UNIX Version 4.0F release. This restriction can reduce performance for certain database applications.

The following error message on the system's console terminal (also logged in /var/adm/messages) indicates possible performance loss for applications using GH chunks:

```
gh_chunks value of # invalid
```

where # is a number that varies depending on memory size.

To remove the GH chunks restriction, you need to modify your target kernel configuration file (and rebuild the kernel) and change the state of a console firmware environment variable. To make these changes, follow these steps:

1. Follow the steps in Section 4.5.3 of the *Guide to System Adminstration*, with the following exceptions:

   In step 4, edit the configuration file and add the following line immediately before the first line starting with makeoptions:

   ```
   makeoptions LOADADDR="fffffc0000430000"
   ```

   In step 6, instead of /usr/sbin/shutdown -r now, add the following line:

   ```
   /usr/sbin/shutdown -h now
   ```

2. Check the console firmware version:

```
P00>>>show version
```

If the version is not Version 5.5 or later, you need to upgrade your firmware to Version 5.5 or later.

3. Change the value of the `console_memory_allocation` environment variable from `old` to `new` and reset the system:

   ```
   P00>>>set console_memory_allocation new
   ```

   ```
   P00>>>init
   ```

4. Boot the new kernel:

   ```
   P00>>>boot
   ```

   If the new kernel fails to boot use one of the following procedures:

   ```
   P00>>>set console_memory_allocation old
   ```

   ```
   P00>>>init
   ```

   ```
   P00>>>boot -fi vmunix.save
   ```

   or:

   ```
   P00>>>boot -fi genvmunix
   ```

   Correct the error and repeat the previous procedure.

Additional Information

- If you encounter the following error message, you have most likely attempted to boot a kernel with the old load address:

  ```
  Bootstrap address collision, image loading aborted
  ```

  To boot old kernels:

  ```
  P00>>>set console_memory_allocation old
  ```

  ```
  P00>>>init
  ```

  ```
  P00>>>boot
  ```

  Note

  The generic kernel (`/genvmunix`) will boot with `console_memory_allocation` set to old or new.

- The patch kit installs a new `/usr/sbin/sizer` command. If you rebuild the kernel using Section 4.5.1 or 4.5.2 of the *System Administration Manual*, the new sizer will automatically adjust the kernel's load address.

  Note

  If you customized your existing configuration file, `doconfig` allows you to edit the new configuration file so you can restore your customizations.

2

Summary of Base Operating System Patches

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

Table 2–1 provides a summary of patches.

Table 2–1: Summary of Base Operating System Patches

Patch IDs	Abstract
Patch 3.00 OSF440CDE-003	**Patch:** Security (SSRT0585U) **State:** Existing A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. HP has corrected this potential vulnerability.
Patch 7.00 OSF440DX-001	**Patch:** dxcalendar Reminder Displays Through dxpause Screen **State:** Existing This patch fixes the problem where the dxcalendar reminder displays through the pause screen (dxpause) and remains on the top of the pause window.
Patch 8.00 OSF440-010	**Patch:** Fix For POP Mail Handler **State:** Existing This patch corrects the following: • Netscape Mail clients are unable to access their mailboxes after an initial session. The /usr/spool/pop/username.lock file is left over and must be removed manually. • The POP mail handler fails to properly rename its temp file after receiving a quit command.
Patch 11.00 OSF440-013	**Patch:** Security (SSRT0596U) **State:** Existing A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. HP has corrected this potential vulnerability.
Patch 19.00 OSF440-020	**Patch:** Fix for yacc **State:** Existing This patch fixes a problem in yacc that causes it to generate parse tables that result in the parser not executing a user-specified error recovery action. If a yacc specification worked in Version 3.2 and no longer works in Version 4.0, this may be the problem.
Patch 36.00 OSF440-041	**Patch:** volrootmir -a Cmd Fails **State:** Existing This patch fixes a problem where the LSM command volrootmir -a fails if the source and target disks are not the same type.
Patch 37.00 OSF440-042	**Patch:** volrecover Not Returning Failed Status Code **State:** Existing This patch corrects a problem in which a failure of the volrecover utility will not return a failed status code.

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

Patch 38.00 OSF440-043	**Patch:** quotaon Returns Incorrect Error Status **State:** Existing This patch fixes a problem in which the quotaon command returned an incorrect error status if the file system did not exist.
Patch 60.00 OSF440-008	**Patch:** Fix for spo_misc_errors errlog Entries **State:** Existing This patch fixes the cause of the spurious spo_misc_errors errlog entry on 4100 class systems.
Patch 61.00 OSF440X11-001	**Patch:** Enhancement for makedepend Utility **State:** Existing This patch increases the maximum number of files that one file can depend on in the makedepend utility from 1024 to 4096.
Patch 68.00 OSF440-047B	**Patch:** nroff Incorrectly Translates Years After 1999 **State:** Existing This patch fixes a Y2K problem with the nroff text formatter in which the years after 1999 are translated to be 19xxx with xxx being the number of years that have passed since 1900. In this case, the year 2010 displays as 19110.
Patch 75.00 OSF440-060B	**Patch:** chvol Read and Write Transfer Size Increased **State:** Existing This patch corrects the following: • AdvFS volumes were not setting the default I/O byte transfer size to the preferred size reported by the disk drives. • AdvFS chvol read and write transfer size range was increased. • The read-ahead algorithm was modified to improve performance under certain conditions.
Patch 76.00 OSF440-001	**Patch:** Fix for simple lock panic **State:** Existing This patch fixes a system panic with the following panic string: simple_lock: time limit exceeded
Patch 82.00 OSF440-106	**Patch:** Fix for system crash **State:** Existing This patch fixes a problem in which the system was consistently crashing when the user pressed keys during the transition from firmware callback to OS console handling.
Patch 101.00 OSF440-126	**Patch:** Fix for prof -pixie -asm command **State:** Supersedes patch OSF440-122B (202.00) This patch corrects the following: • Fixes the name demangling for the tools that print symbol table names generated by the C++ V6.2 compiler. This problem will only occur for most C++ objects compiled with the ANSI options. • Fixes a problem where prof -pixie -asm would dump core if the executable being profiled contained extremely long symbol names.
Patch 127.00 OSF440-153	**Patch:** Security (SSRT0583Z) **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. HP has corrected this potential vulnerability.

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

Patch 148.00 OSF440-069	**Patch:** Fix for rsh hang **State:** Existing This patch fixes rsh(1) hanging forever in select().
Patch 153.00 OSF440-074	**Patch:** Fixes a problem within the SCSI and tape subsystems **State:** Existing This patch fixes a problem within the SCSI and tape subsystems, in which an expression was not being evaluated properly.
Patch 162.00 OSF440-083	**Patch:** Fix for unresolved symbol:scc_configure message **State:** Existing This patch fixes a problem in which systems that use Compaq Tru64 UNIX and install DECnet/OSI and WDD would get the following error message when attempting to build a kernel: unresolved symbol:scc_configure
Patch 170.00 OSF440-091	**Patch:** Fixes a problem with the stdhosts command **State:** Existing This patch fixes a problem with the stdhosts command when the file processed has lines longer than 256 characters. The error message “stdhost:malformed line ignored” is displayed.
Patch 179.00 OSF440-192	**Patch:** Fix for panics on AlphaServer GS140/GS60 systems **State:** Supersedes patch OSF440-002 (18.00) This patch corrects the following: • Resolves corrupt EV6 binary error log entries for IOP detected UDE (Uncorrectable Data Error) packets on AlphaServer 8200/8400 platforms. • Fixes a problem on some AlphaServer GS140/GS60 configurations where a simple lock timeout or TB shoot ack timeout panic may occur.
Patch 182.00 OSF440CDE-010	**Patch:** Fix for X server color map problem **State:** Existing This patch fixes a problem where there were no available colors in the X server’s color map after the CDE screen lock was displayed.
Patch 183.00 OSF440CDE-011	**Patch:** Security (SSRT0614U) **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. HP has corrected this potential vulnerability.
Patch 188.00 OSF440DX-003	**Patch:** Compaq SCSI SNMP sub-agent returns incorrect info **State:** Existing This patch fixes a problem that causes the Compaq SCSI SNMP subagent (cpq_mibs) to often return incorrect SCSI CD-ROM and tape devices model information, which results in invalid information displaying on the Insight Management web pages.
Patch 194.00 OSF440DX-009	**Patch:** Security (SSRT0612U) **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. HP has corrected this potential vulnerability.

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

Patch 196.00 OSF440X11-006	**Patch:** XDMCP Indirect queries do not work **State:** Existing This patch fixes a problem in the X Display Manager (xdm) where XDMCP Indirect queries do not work.
Patch 198.00 OSF440X11-008	**Patch:** X server crashes when viewing TIFF images **State:** Existing This patch fixes a problem where viewing certain TIFF images with an image viewer crashed the X server.
Patch 205.00 OSF440CDE-009B	**Patch:** Fix for dxaccounts BadPixmap error **State:** Existing This patch fixes a problem where the Account Manager application, dxaccounts, gets a “BadPixmap” error when selecting an account after the “View Preferences” “Display Icons By Name” option has been selected.
Patch 209.00 OSF440-131B	**Patch:** Static library fix for libclass.a **State:** Existing This patch fixes a class_admin/class_daemon problem. When a PID is added to a class it cannot be removed from the class scheduler until the process terminates or the class_scheduler has been stopped.
Patch 211.00 OSF440CDE-012	**Patch:** Security (SSRT0615U) **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. HP has corrected this potential vulnerability.
Patch 215.00 OSF440DX-012	**Patch:** checklist utility does not provide scroll bar **State:** Existing This patch fixes a problem where the checklist utility did not provide a scroll bar on higher resolution displays (1600x1200).
Patch 216.00 OSF440DX-013	**Patch:** diskconfig may display incorrectly **State:** Existing This patch fixes a problem where the Disk Configuration Manager application, diskconfig, displayed incorrectly on some non-Compaq X servers. The font used for menu items was incorrect so that the menus contained random symbols instead of text.
Patch 221.00 OSF440X11-017	**Patch:** Fixes problem on systems with a Powerstorm 4D10T **State:** Existing This patch fixes a problem where, on systems with a Powerstorm 4D10T (ELSA GLoria Synergy) graphics board, sometimes the X server did not draw lines correctly.
Patch 232.00 OSF440-172	**Patch:** Fix for lex command **State:** Existing This patch fixes a problem in lex that causes it to generate incorrect tables. This results in the lexical analyzer failing to recognize some kinds of regular expressions involving exclusive start states.
Patch 233.00 OSF440-173	**Patch:** Fix for ris script **State:** Existing This patch corrects the following problems with the /usr/sbin/ris script: • It incorrectly queried the user for a gateway to be used to serve a specific client when no gateway was required. • It could fail if no default route had been established.

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

Patch 237.00 OSF440-179	**Patch:** defragment incorrectly reports large free space holes **State:** Supersedes patch OSF440-029 (26.00) This patch corrects the following: • Fixes a problem with the defragment command, where the -V option is not being parsed properly. • Fixes the defragment program to properly report on extremely large (>4.3GB) free space holes. Previously it would report free space percentages larger than 100% and would add these large holes to the smallest range (<100K) instead of the largest range (>10M) where they belong.
Patch 242.00 OSF440-185	**Patch:** Fix for news command **State:** Existing This patch fixes a problem in which the news command fails due to the appending of additional characters to file names in the /usr/news directory.
Patch 243.00 OSF440-186	**Patch:** Fix for rpc.statd hang **State:** Existing This patch fixes a problem where rpc.statd hangs as it tries to notify dead remote systems.
Patch 256.00 OSF440-205	**Patch:** mkfdmn command does not report errors **State:** Existing This patch corrects a problem that resulted in the mkfdmn command not reporting errors if the user attempted to create a volume with a name that is more than 31 characters long.
Patch 262.00 OSF440-217	**Patch:** lprsetup command sets up printers incorrectly **State:** Existing This patch fixes a problem where the lprsetup command would incorrectly set up certain types of printers, such as the HP1120c, HP4000tn, or HP61.
Patch 281.00 OSF440-245	**Patch:** Fix for tmv2_notify_cbf problem **State:** Supersedes patches OSF440-006 (53.00), OSF440-165 (226.00), OSF440-234 (273.00) This patch corrects the following: • Fixes a panic that occurs when KZPSA resources are not available to re-enable a channel or a device after a bus reset. The panic string is: panic("(spo_process_rsp) ran out of memory!") • Fixes a problem with the KZPSA driver. A timer is not being canceled causing a panic with the following error message: xpt_callback: callback on freed CC • Fixes a problem in which the system can panic with the following message: KZPSA PANIC SPO_RET_CARRIER:CARRIER NOT IN USE • Fixes a problem with tmv2_notify_cbf messages being logged from KPBSA adapters and creating very large binary.errlog files in a clustered environment.

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

Patch 296.00 OSF440-261	**Patch:** Fix for compress utility **State:** Existing This patch corrects a problem with the (un)compress utility that could result in either an incomplete compressed file and loss of the original uncompressed file, or an incomplete uncompressed file and loss of the original compressed file.
Patch 297.00 OSF440-262A	**Patch:** Fix for voldisksetup, voldiskadd, and newfs **State:** Existing This patch fixes problems with the voldisksetup, voldiskadd, or newfs commands. Each will report device errors while checking for overlapping partitions where there is no overlap on that particular device.
Patch 299.00 OSF440-264	**Patch:** Fix for update installation hang **State:** Existing This patch fixes a problem in which a hang can occur during update install.
Patch 306.00 OSF440-271	**Patch:** Fixes Standards namespace pollution problem **State:** Existing This patch corrects some Standards namespace pollution.
Patch 308.00 OSF440-273	**Patch:** Corrects an NIS client problem **State:** Existing This patch corrects a problem where an NIS client has a different shell listed for an NIS user than does the server. When the users tried to change their NIS passwords, the password change failed, but the shell was updated.
Patch 313.00 OSF440-279	**Patch:** showfdmn may core dump **State:** Existing This patch fixes a problem in which advfs showfdmn would sometimes core dump.
Patch 315.00 OSF440-282	**Patch:** Fixes performance problem on LSM mirrored volumes **State:** Existing This patch fixes a performance problem for round robin sequential reads on LSM mirrored volumes.
Patch 323.00 OSF440-291	**Patch:** Various fixes for ALPHAVME320 systems **State:** Supersedes patch OSF440-108 (84.00) This patch corrects the following: • Fixes two problems on the ALPHAVME320 platform: – Data corruption in the VB Backplane driver. – No floppy support in the platform code. Following is the error message received during the boot when the floppy is configured at irq6: EBV16, invalid isa0 irq6 • Fixes three problems in the existing VB VME Backplane Driver running on AlphaVMExx platforms: – VB VME Backplane Driver does not configure when the sysconfigtab parameter, VB_MAXNODES, is less than 10. – VB VME Backplane Driver hangs and the nodes lose liveness when the sysconfigtab parameter, VB_MAXNODES, is equal to 2. – VB VME Backplane Driver Performance is unacceptable for customer applications.

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

Patch 337.00 OSF440-168B	**Patch:** Fix for AdvFS property list handling **State:** Existing This patch corrects two problems in AdvFS property list handling: • Creation of property lists entries in AdvFS filesets with no available mcells will result in kernel memory fault (kmf). • The get_proplist_entry function (used to disassemble the property list buffer returned by the getproplist system call) returned the incorrect name length on property list names longer than 127 characters.
Patch 339.00 OSF440-262B	**Patch:** voldisksetup incorrectly reports device errors **State:** Existing This patch fixes problems with voldisksetup, voldiskadd, or newfs commands. Each will report device errors while checking for overlapping partitions where there is no overlap on that particular device.
Patch 341.00 OSF440CDE-018	**Patch:** Fixes file permission problem for trashinfo file **State:** Supersedes patches OSF440CDE-005 (5.00), OSF440CDE-007 (184.00) This patch corrects the following: • Fixes a problem where the CDE File Manager (dtfile) sometimes left defunct processes. • Fixes a problem where the Common Desktop Environment (CDE) File Manager (dtfile) did not work correctly in restricted mode. • Fixes a problem in which file permissions allow any user to write to the /.dt/Trash/.trashinfo file.
Patch 344.00 OSF440CDE-021	**Patch:** Security (SSRT0580U) **State:** Supersedes patch OSF440CDE-004 (4.00) This patch corrects the following: • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. HP has corrected this potential vulnerability. • Fixes a problem where the Common Desktop Environment (CDE) Application Manager did not recreate the list of application groups at login. After customizing the application groups, users would see the old groups instead of the new groups.

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

Patch 351.00 OSF440X11-021	**Patch:** Provides missing compose definitions **State:** Supersedes patches OSF440CDE-014 (212.00), OSF440CDE-017 (340.00), OSF440X11-019 (223.00) This patch corrects the following: • Adds the ISO8859-15 functionality to the main Xresource file on the system and to the specific dtlogin resource file. With these changes, X applications have ISO8859-15 locale support integrated directly into the application. • Adds Catalan (ISO8859-15) to the list of languages from which users can choose when logging in. The additional item identifies the Catalan Latin-9 locale, which supports the Euro currency sign. • Implements Xlocales definitions that allow X applications to run under the ISO8859-15 locales. Using ISO8859-15 locales allows users to enter and use newly defined ISO8859-based characters such as the Euro monetary symbol. • Provides missing compose definitions when in ISO8859-15 based locales for the scaron, Scaron, zcaron, and Zcaron characters.
Patch 353.00 OSF440X11-023	**Patch:** Fix for Turkish F keyboard problem **State:** Existing This patch fixes the Turkish F keyboard problem, where the characters Ccedilla and ccedilla cannot be entered from the keyboard directly.
Patch 358.00 OSF440X11-028	**Patch:** X server incorrectly includes DPSExtension **State:** Existing This patch fixes a problem where the X server would include the Adobe Display PostScript extension (Adobe-DPS-Extension, DPSExtension) in its response to a ListExtensions request even though Display PostScript is not supported in Tru64 UNIX V4.0F.
Patch 381.00 OSF440-327	**Patch:** Security (SSRT0624U) **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. HP has corrected this potential vulnerability.
Patch 390.00 OSF440-339	**Patch:** Prevents vold from core dumping **State:** Existing This patch prevents /sbin/vold from dumping core during an execution of a volprint or other query command.
Patch 395.00 OSF440-344	**Patch:** mdir command displays year 2000 date incorrectly **State:** Existing This patch fixes a problem in which the mdir command displays the date incorrectly for the year 2000.
Patch 402.00 OSF440-351	**Patch:** Fixes hang in 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 405.00 OSF440-354	**Patch:** Fixes a tftpd problem **State:** Existing This patch fxes a tftpd problem when responding to a broadcast read request, and adds the -b option to control whether to respond to any broadcasts.

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

Patch 406.00 OSF440-355	**Patch:** Fixes a kernel memory fault when using ATM **State:** Supersedes patch OSF440-316 (374.00) This patch corrects the following: • Fixes a problem in the ATM atm_cmm_connect API routine when trying to create a VC. • Fixes a kernel memory fault when using ATM.
Patch 409.00 OSF440-358	**Patch:** Fixes a problem with NCR810 script **State:** Existing This patch fixes a problem with the NCR810 script that can cause the KZPAA/NCR810 to hang.
Patch 420.00 OSF440-369	**Patch:** quotactl prototype is now POSIX compliant **State:** Supersedes patch OSF440-137 (111.00) This patch corrects the following: • Fixes a problem where the system can panic with a "kernel memory fault" in dqget. • Changes the quotactl prototype in /usr/include/ufs/quota.h to meet POSIX standards.
Patch 435.00 OSF440-385A	**Patch:** Adds missing prototype for stime function **State:** Existing This patch adds the missing prototype for the stime() function to <sys/time.h>, allowing C++ programs and other software to properly resolve it.
Patch 443.00 OSF440-395	**Patch:** Danish locale now uses all lowercase month names **State:** Existing This patch updates the Danish (da_DK.ISO8859-1) locale to use all lowercase month names.
Patch 447.00 OSF440-399	**Patch:** Fixes a problem with the psiop driver **State:** Supersedes patch OSF440-163 (225.00) This patch corrects the following: • Fixes a panic when using the scu command. When formatting a floppy using the scu command the system panics with the following error message: System Uncorrectable Machine Check 660 (retry set) • Fixes a problem with the psiop driver that causes it to fail when vdump is used. The following error is displayed: vdump : unable to write to device

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

Patch 450.00 OSF440-402	**Patch:** Fixes several DEC C compiler problems **State:** Supersedes patches OSF440-134 (108.00), OSF440-293 (325.00) This patch corrects the following: • A compiler problem that allowed the generation of EV67 (CIX) instructions to be generated when using the -arch ev6 switch. • A compile time performance problem with a very large (1.6 MB) array initialization. • An optimization problem that caused incorrect output when using a signed char in a strcpy-like routine, if compiled using -O4 or higher. • A compile-time error for a source line such as a = strcpy(b,c) + 7. • An optimizer problem that caused an unintended sign-extension in the Perl program. This caused an "op/pack" failure in test 9. • A compiler crash when compiling Xemacs 21.1.4 with -O4. • An optimizer problem in loop unrolling that suppressed intermediate updates to induction variables under certain conditions. • A particular short parameter assignment caused incorrect run-time result. • An assignment of type k = (char)(l >> 8) was not sign-extended. • An optimizer problem that produced incorrect code when certain bounds checking within a loop was moved outside the loop. • An optimizer problem that caused the wrong result when compiled at -O2, under certain conditions. • A virtual memory exhausted error when compiling the Open Source encryption library OpenSSL. • A compiler crash under certain conditions that produces an “Assertion failure: Non-Arithmetic Data Type” error.
Patch 461.00 OSF440-416	**Patch:** Cursor is displayed incorrectly **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.
Patch 469.00 OSF440X11-025B	**Patch:** Fix for X server interaction with X font server **State:** Existing This patch fixes various problems with the X font server and with the X server’s interaction with X font servers.
Patch 470.00 OSF440X11-025C	**Patch:** Problem with X server interaction **State:** Supersedes patch OSF440X11-003 (63.00) This patch corrects the following: • Fixes a problem where the X font server (xfs) sometimes failed with a segmentation fault when it received an invalid request. • Fixes various problems with the X font server and with the X server’s interaction with X font servers.
Patch 474.00 OSF440-385B	**Patch:** stime function does not compile under C++ **State:** Existing This patch adds the missing prototype for the stime() function to <sys/time.h>, allowing C++ programs and other software to properly resolve it.

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

Patch 475.00 OSF440-425	**Patch:** Fixes kernel panic occuring in lockmode 4 **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 476.00 OSF440-411B	**Patch:** Performance issues on EV6 SMP machines **State:** Supersedes patch OSF440-054B (71.00) This patch corrects the following: • Fixes problems in the DECthreads library for Tru64 UNIX. Included in this patch are changes to support Ladebug enhancements and a bug fix for applications which employ SCS threads of different priorities. • Addresses performance and scalibility issues for highly contended threaded applications running on EV6 SMP machines.
Patch 478.00 OSF440-437	**Patch:** Fix for LAT driver **State:** Existing 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 480.00 OSF440-488	**Patch:** Extends max length of identifier for assembler **State:** Supersedes patch OSF440-365 (416.00) This patch corrects the following: • Resolves a problem that caused the assembler to flag any identifiers whose length exceeded 1024 characters with an assembly-time error. With this patch, such identifiers are now accepted. • Corrects a problem where the assembler would generate incorrect error messages for source programs that produce a mix of hand-coded and assembler-generated relocation operands.
Patch 482.00 OSF440-459	**Patch:** Fix for mailx problem **State:** Existing This patch corrects the problem so mailx(1) will work correctly if the -r and -s flags are used together.
Patch 507.00 OSF440-436B	**Patch:** NFS writes cause protocol violations **State:** Existing This patch fixes reply values for NFS writes which were causing protocol violations.
Patch 526.00 OSF440-461	**Patch:** Fix for kernel memory fault **State:** Existing This patch fixes a kernel memory fault that affects linear machines such as ebm30, GS160 through GS320, DS10, DS20, ES40, and XP1000.
Patch 530.00 OSF440-441	**Patch:** Fix for Y2K lastlogin command problem **State:** Existing This patch resolves the Y2K problem of lastlogin command incorrectly calculating the last date each user logged in.

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

Patch 537.00 OSF440CDE-024	**Patch:** Security (SSRT0600U) **State:** Supersedes patches OSF440CDE-006 (6.00), OSF440CDE-008 (185.00), OSF440CDE-025 (535.00) This patch corrects the following: • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. HP has corrected this potential vulnerability. • Fixes a problem where dtlogin may incorrectly set the permissions of /var to 775. It also fixes a problem where dtlogin may incorrectly set the umask to 002 for csh users. • Fixes a problem with the Common Desktop Environment (CDE) login process where, if you selected the Command Line Login option and logged in, sometimes the CDE login screen would be redisplayed before you had logged out. • Fixes a problem where the Common Desktop Environment (CDE) login daemon, dtlogin, core dumps occasionally when servicing requests from XDMCP clients such as X terminals or PCs running X servers.
Patch 548.00 OSF440-438	**Patch:** Fix for advscan **State:** Existing This patch fixes a problem where advscan -a -g does not display bootable partitions properly.
Patch 561.00 OSF440-428	**Patch:** Fix for system panic **State:** Existing This patch fixes a problem where encoding for the SysV Open call audit parameter was incorrect. This could cause a system panic.
Patch 567.00 OSF440-439B	**Patch:** Security (SSRT0642U) **State:** Supersedes patches OSF440-149B (203.00), OSF440-251B (338.00), OSF440-301B (472.00), OSF440-370B (473.00), OSF440-462B (565.00) This patch corrects the following: • Fixes a problem of libsecurity producing a core file when handling error conditions. • 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. HP has corrected this potential vulnerability. • Corrects a problem of the rsh command displaying a warning message instead of the rsh command output when C2 security is configured. • 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 when a system is configured with DECnet, C2, and NIS. When invoking edauth(8) <user_name>, the error “Must be on NIS master server to update entry for <user_name>” is returned.

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

Patch 592.00 OSF440-507	**Patch:** Fixes a problem with floppy driver **State:** Supersedes patch OSF440-366 (417.00) HP 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 HP 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.
Patch 598.00 OSF440-430	**Patch:** Fix for tapex utility **State:** Existing This patch fixes several problems in the tapex utility; • Accuracy of performance tests has been improved. • The tapex exit status has been corrected. • The tapex utility was fixed to determine eom status in Command Timeout Test and exit with non-0 status to indicate failure.
Patch 642.00 OSF440-544B	**Patch:** Support for activating temporary data logging **State:** Supersedes patch OSF440-296 (361.00) This patch fixes a problem in which the chfile utility returns an incorrect error code. This patch provides support for activating temporary data logging on a mount point.
Patch 646.00 OSF440DX-023	**Patch:** Updates Netscape Communicator to Version 4.76 **State:** Existing This patch updates Netscape Communicator to Version 4.76 to fix missing default MIME types in Netscape Communicator Version 4.75.
Patch 668.00 OSF440-513	**Patch:** ATM setup script fails when configuring ELAN **State:** Existing This patch fixes a problem of the ATM setup script failing when configuring an elan if the lane subsystem is not loaded.

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

Patch 670.00 OSF440-572	**Patch:** Incorrect heartbeat timer in memory channel driver **State:** Supersedes patches OSF440-118 (94.00), OSF440-403 (451.00) This patch corrects the following: • Fixes an incorrect heartbeat timer within the memory channel driver which caused rail failures to be incorrectly reported on memory channel Version 2 cards. With the heartbeat timer set too short, the system can be erroneously led to believe a hardware failure has occurred. Messages of the form "rmerror_int: ..." are output to the messages file containing an error_type which has bit 29 set in error_type (heartbeat timeout). The binary error log will also have this data. Typically, the error_type data will be 0xe00000000. The messages are followed by the system hanging or panicing. When panicking, the following message is produced: panic (cpu 0): rm_failover_if_necessary, both rails bad A real hardware failure produces the same symptoms and stack trace. For example, having an error_type of 0xe00000002 indicates a write transmit hardware fatal failure. • Fixes a problem where an MC1 or 1.5 will not configure with an EV6 8x00. It also improves error handling with MC 2 in a Virtual Hub. • Fixes a problem in the memory channel driver which could result in panics with rm - inconsistent local spinlock structures being logged.
Patch 672.00 OSF440X11-041A	**Patch:** Fix for pixel problem for CDE **State:** Existing This patch fixes the problem of erroneous pixels left behind when dragging CDE application manager icons on the desktop.
Patch 676.00 OSF440-516	**Patch:** Fix for newgrp command **State:** Existing This patch corrects the problem where newgrp(1) fails if the file /etc/group contains multiple lines for one group.
Patch 684.00 OSF440-537	**Patch:** Fixes automount handling of nogrpid option **State:** Supersedes patch OSF440-024 (22.00), OSF440-377 (427.00) This patch corrects the following: • Fixes a problem in which the automount daemon hangs when invoked by the rsh command. • Prevents the message "nfscast: select: Invalid argument" message from appearing in the daemon.log when the server is not available. It also changes the "trymany: servers not responding: RPC: Unable to receive " message to an informational vs. error message. • Fixes the automount handling of the nogrpid option.
Patch 690.00 OSF440CDE-028A	**Patch:** Fix for dtpad **State:** Supersedes patch OSF440CDE-009A (186.00) This patch corrects the following: • Fixes a problem where the Account Manager application, dxaccounts, gets a “BadPixmap” error when selecting an account after the “View Preferences” “Display Icons By Name” option has been selected. • Fixes a problem where, if dtpad cannot allocate enough memory, it will exit and leave a zero-length file in place of the file being edited.

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

Patch 705.00 OSF440-506	**Patch:** fixso command may cause segmentation fault **State:** Existing This patch fixes a problem with the /usr/ucb/fixso command that can cause a segmentation fault.
Patch 707.00 OSF440-511	**Patch:** Fix for bindsetup problems **State:** Existing This patch fixes several problems when bindsetup is used to change hostnames.
Patch 718.00 OSF440DX-022	**Patch:** dop cannot find application names containing period **State:** Existing This patch fixes a problem in which dop (division of privileges) cannot find application names which contain a "." (dot) in them. For example, a name such as sysmon.csh.
Patch 725.00 OSF440-517	**Patch:** Security (SSRT0672U) **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. HP has corrected this potential vulnerability.
Patch 727.00 OSF440-575	**Patch:** Fix for Korn shell hang **State:** Existing 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 729.00 OSF440X11-037	**Patch:** Fixes a memory leak in the X server **State:** Supersedes patch OSF440X11-027 (357.00) This patch corrects the following: • Fixes a problem where the X server could core dump or get unaligned access errors when clients used the Multi-Buffering extension. • 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).
Patch 735.00 OSF440-523	**Patch:** Prevents Turbolaser panic with DE600 in pci slot 0 **State:** Existing This patch prevents a panic on TurboLaser systems with a DE600 in pci slot 0. Mis-identification of the DE600 in pci slot 0 causes data structure corruption. TurboLaser systems include the following: AlphaServer 8200 AlphaServer 8400 AlphaServer GS60 AlphaServer GS60E AlphaServer GS140 A DE600 is a single-port 10/100 Mbps Fast Ethernet NIC.
Patch 737.00 OSF440CDE-028B	**Patch:** dtpad does not allocate enough memory **State:** Existing This patch fixes a problem where, if dtpad cannot allocate enough memory, it will exit and leave a zero-length file in place of the file being edited.

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

Patch 739.00 OSF440-564	**Patch:** Security (SSRT1-15, SSRT0713U) **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. HP has corrected this potential vulnerability.
Patch 741.00 OSF440-519	**Patch:** Security (SSRT0592U) **State:** Supersedes patches OSF440-241 (279.00), OSF440-287 (319.00) This patch corrects the following: • Fixes a problem with rdist(1) which consumes huge amounts of memory, and when there are a lot of symlinks in the fileset, it can simply fail to fully populate the remote site, or cause low-memory problems on the local machine. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. HP has corrected this potential vulnerability. • Corrects a problem in the rdist utility which was causing segmentation faults on files with more than one link.
Patch 783.00 OSF440-590B	**Patch:** Fix for incorrect available size for AdvFS domain **State:** Supersedes patches OSF440-040 (35.00), OSF440-183 (240.00), OSF440-330 (384.00), OSF440-585B (644.00) This patch corrects the following: • Allows the /sbin/advfs/verify utility to detect loops in the list of free frags kept in the frags file. • Avoids corruption of a file system when verify runs with -r and -f flags on an active domain. Verify returns usage message when -r flag is used with either -f or -d. • Fixes the following /sbin/advfs/verify command problems: – verify fails to complete on a large number of files. – verify will core dump when an offset into mountd[] array that is used to pull out the fileset name is corrupted. – verify incorrectly reports errors on BMTs that have multiple extent records for domains created with the mkfdmn -p switch. – verify fails when lseeking on very large domains. • 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. • Corrects an AdvFS problem where an on-disk variable wraps when more than 64K metadata entries are required to map the disk blocks of a file or metadata file. The side effects of this problem were data inconsistencies and an incorrect available size for the domain.

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

Patch 796.00 OSF440-639	**Patch:** Fixes a problem in latsetup **State:** New This patch fixes a problem in latsetup when the directory /dev/lat is not found.
Patch 801.00 OSF440-641B	**Patch:** Security (SSRT1-40U, SSRT1-41U, SSRT1-42U, SSRT1-45U) **State:** New A potential security vulnerability has been discovered where, under certain circumstances, users can clobber temporary files created by shell commands and utilities (for example, under /sbin, /usr/sbin, /usr/bin, and /etc). HP has corrected this potential vulnerability.
Patch 817.00 OSF440-598	**Patch:** Fix for ccmn_rem_ccb3 panic **State:** Supersedes patches OSF440-025 (136.00), OSF440-247 (283.00), OSF440-281 (314.00) This patch corrects the following: • Fixes callback thread blocking forever in isp_enable_lun. • Fixes assert wait in xpt_ccb_alloc panic. • Fixes a problem on configurations having multiple Qlogic 1020/1040 based SCSI controllers (for example KZPBAs) and multiple CPUs. The problem could result in stalled I/O. This could be seen as a performance degradation, command timeouts, or, in the worse cases, a system hang condition. • Fixes callback on freed CCB panics. • Fixes a bug that causes a "ccmn_rem_ccb3: ccb not on any list" cluster node panic.
Patch 823.00 OSF440X11-042A	**Patch:** Security (SSRT0638U) **State:** Supersedes patch OSF440X11-020A (350.00) This patch corrects the following: • Fixes a problem in which the svn widget of libDXm.so creates identical backgrounds and foregrounds. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of root directory compromise via lpr using X11.
Patch 827.00 OSF440-614	**Patch:** Security (SSRT1-85U) **State:** New A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. xntpd contains a potential buffer overflow that may allow unauthorized access to bin privileges. HP has corrected this potential vulnerability.
Patch 829.00 OSF440-594	**Patch:** Fix for i2c lock hierarchy violation **State:** Supersedes patches OSF440-145 (119.00), OSF440-555 (697.00) This patch corrects the following: • Fixes a intermittent hang occurring in the i2c code. This hang is most commonly seen on the DS10 workstation. • Fixes DS10/DS20 performance problems introduced with the i2c driver by using thread blocking, rather than event_meout() and DELAY(). • Fixes a lock hierarchy violation that could be seen with the generic kernel attribute lockmode turned on.

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

Patch 845.00 OSF440-643	**Patch:** Fix for dropped ATM lane connections **State:** Supersedes patches OSF440-068 (147.00), OSF440-356 (407.00), OSF440-429 (584.00) This patch corrects the following: • Fixes a problem with the creation of multiple ATM ELANS. • Fixes a problem in which the system may panic with the error message "Unaligned kernel space access from kernel mode" when running ATM ELANs. • When running ATM LAN Emulation, using more than four ATM NetRAIN interfaces can result in recursive calls causing a “kernel stack not valid” halt. • Corrects a problem which could result in ATM/lane connection requests being dropped.
Patch 849.00 OSF440-610	**Patch:** Fix for telnet and ftp commands **State:** New This patch fixes a problem that occurs with the telnet and ftp commands. Telnet or ftp processes that are no longer in use are left on the system indefinitely. When a user tries to log in, the login process hangs after displaying the last login message.
Patch 851.00 OSF440-623	**Patch:** Miscellaneous joind fixes **State:** Supersedes patches OSF440-079 (158.00), OSF440-201 (253.00), OSF440-246 (282.00), OSF440-249 (285.00), OSF440-538 (746.00) This patch corrects the following: • Adds an error message to DHCP to inform a user that they may be using an outdated database. The message also points to the README for database conversion instructions. • Fixes a problem of the joind daemon not appending the hostname to the load file specified in the bf flag in the /etc/bootptab file. • Fixes a problem in which joind does not listen on interfaces configured with DECnet and returns "unaligned access" messages. • Fixes a problem in which bprelay does not work properly and displays the following error message: bprelay[658]: can’t find interface which received packet • Corrects a problem with joind which caused it to respond to certain client dhcp requests via the wrong port. • Fixes a problem where joind may fail to clean up its lock files in /var/join.
Patch 855.00 OSF440X11-042B	**Patch:** Security (SSRT0638U) **State:** Supersedes patches OSF440X11-020B (468.00) This patch corrects the following: • Fixes a problem in which the svn widget of libDXm.so creates identical backgrounds and foregrounds. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of root directory compromise via lpr using X11.

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

Patch 1062.00 OSF440-839	**Patch:** Security (SSRT0556U, SSRT2275) **State:** Supersedes patches OSF440-030 (28.00), OSF440-686 (1058.00), OSF440-984B (1059.00), OSF440-885 (1060.00) This patch corrects the following: • A potential security vulnerability has been discovered where, under certain circumstances users may gain unauthorized access. HP has corrected this potential vulnerability. • Fixes a problem in uucp. uucp between two Tru64 UNIX boxes hangs when a uucp failure occurs. • Provides protection against a class of potential security vulnerabilities called buffer overflows. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege. This patch allows a system administrator to enable memory management protections that limit potential buffer overflow vulnerabilities. • 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. HP has corrected this potential vulnerability. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised when a buffer overflow occurs in the uucp utility. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege. HP has corrected this potential vulnerability.
Patch 1065.00 OSF440-766	**Patch:** Fix for kdbx **State:** Supersedes patches OSF440-104B (201.00), OSF440-117 (93.00), OSF440-934B (1063.00) This patch corrects the following: • Fixes a problem with kdbx. A core file created by kdbx was left in the root directory when recovering from a system crash. • Fixes a problem with kdbx. The trace command was showing all threads of a process when using the option that should show only selected threads. • Fixes a problem with audit data not being displayed by audit tool, problems with file object selection/deselection and directories, and NUMA performance issues associated with auditing. • Fixes a premature termination of the ofile kdbx extension, and token length warnings when kdbx is invoked.

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

Patch 1068.00 OSF440-984C	**Patch:** Security (SSRT2275) **State:** Supersedes patch OSF440-984C (1066.00) This patch corrects the following: • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. HP has corrected this potential vulnerability. • Provides protection against a class of potential security vulnerabilities called buffer overflows. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege. This patch allows a system administrator to enable memory management protections that limit potential buffer overflow vulnerabilities.
Patch 1070.00 OSF440-984D	**Patch:** Security (SSRT2275) **State:** New This patch provides protection against a class of potential security vulnerabilities called buffer overflows. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege. This patch allows a system administrator to enable memory management protections that limit potential buffer overflow vulnerabilities.
Patch 1072.00 OSF440-992B	**Patch:** Scripts in /sbin/init.d now world-readable **State:** New This patch makes start-up scripts in /sbin/init.d world readable.
Patch 1074.00 OSF440-788B	**Patch:** Security (SSRT1-40U, SSRT1-41U, SSRT1-42U, SSRT1-45U) **State:** New A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access. HP has corrected this potential vulnerability.
Patch 1076.00 OSF440-850B	**Patch:** Corrects buffer overflow in dxterm utility **State:** Supersedes patch OSF440-052B (69.00) This patch corrects the following: • The keymap used with curses functionality was not in sync with the table contained in the term.h header file. This change corrects that and enables several non-functioning keys in curses-based applications. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised when a buffer overflow occurs in the dxterm utility. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege. HP has corrected this potential vulnerability.
Patch 1078.00 OSF440-984E	**Patch:** Security (SSRT2275) **State:** New This patch provides protection against a class of potential security vulnerabilities called buffer overflows. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege. This patch allows a system administrator to enable memory management protections that limit potential buffer overflow vulnerabilities.

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

Patch 1080.00 OSF440-992C	**Patch:** Scripts in /sbin/init.d now world readable **State:** New Patch makes start-up scripts in /sbin/init.d world readable.
Patch 1082.00 OSF440-992D	**Patch:** Scripts in /sbin/init.d now world readable **State:** New Patch makes start-up scripts in /sbin/init.d world readable.
Patch 1084.00 OSF440-992E	**Patch:** Scripts in /sbin/init.d now world readable **State:** New Patch makes start-up scripts in /sbin/init.d world readable.
Patch 1086.00 OSF440-984F	**Patch:** Security (SSRT2275) **State:** Supersedes patch OSF440-033B (67.00) This patch corrects the following: • Fixes a problem with the mount command where it sometimes kills other processes. • Provides protection against a class of potential security vulnerabilities called buffer overflows. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege. This patch allows a system administrator to enable memory management protections that limit potential buffer overflow vulnerabilities.
Patch 1088.00 OSF440-850C	**Patch:** Corrects buffer overflow in dxterm utility **State:** New A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised when a buffer overflow occurs in the dxterm utility. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege. HP has corrected this potential vulnerability.
Patch 1090.00 OSF440-810B	**Patch:** Security (SSRT1-41U, SSRT1-42U, SSRT1-45U, SSRT1-48U) **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 access. HP has corrected this potential vulnerability.
Patch 1092.00 OSF440CDE-047	**Patch:** Corrects improper file access **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 access. HP has corrected this potential vulnerability.

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

Patch 1094.00 OSF440-891	**Patch:** Security (SSRT1-40U, SSRT1-41U, SSRT1-42U, SSRT1-45U) **State:** Supersedes patch OSF440-641C (803.00) This patch corrects the following: • A potential security vulnerability has been discovered where, under certain circumstances, users can clobber temporary files created by shell commands and utilities (for example, under /sbin, /usr/sbin, /usr/bin, and /etc). HP has corrected this potential vulnerability. • 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 managment. HP has corrected this potential vulnerability.
Patch 1096.00 OSF440-853	**Patch:** Security (SSRT1-40U, SSRT1-41U, SSRT1-42U, SSRT1-45U) **State:** Supersedes patch OSF440-641D (805.00) This patch corrects the following: • A potential security vulnerability has been discovered where, under certain circumstances, users can clobber temporary files created by shell commands and utilities (for example, under /sbin, /usr/sbin, /usr/bin, and /etc). HP has corrected this potential vulnerability. • 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. HP has corrected this potential vulnerability.
Patch 1098.00 OSF440-975	**Patch:** Corrects improper file or privilege management **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. HP has corrected this potential vulnerability.
Patch 1100.00 OSF440-958A	**Patch:** Threaded applications using XTI/TLI may hang **State:** Supersedes patches OSF440-016A (14.00), OSF440-023A (21.00) This patch corrects the following: • Fixes a problem in which an application using the X/Open Transport Interface (XTI) and the DECnet/OSI transport provider is unable to disconnect a rejected request. • Fixes a streams problem in libxti. The t_getprotaddr() function will cause a memory core dump if either of its second or third argument is NULL. • Fixes a problem in XTI caused by a blocked mutex lock. Any thread attempting to send an abortive disconnect would hang.

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

Patch 1102.00 OSF440-958B	**Patch:** Fix for XTI/TLI static library hang **State:** Supersedes patches OSF440-016B (65.00), OSF440-023B (66.00) This patch corrects the following: • Fixes a problem in which an application using the X/Open Transport Interface (XTI) and the DECnet/OSI transport provider is unable to disconnect a rejected request. • Fixes a streams problem in libxti. The t_getprotaddr() function will cause a memory core dump if either of its second or third argument is NULL. • Fixes a problem in XTI caused by a blocked mutex lock. Any thread attempting to send an abortive disconnect would hang.
Patch 1105.00 OSF440CDE-053A	**Patch:** Security (SSRT1-80U) **State:** Supersedes patches OSF440CDE-029A (785.00), OSF440CDE-054A (1103.00) This patch corrects the following: • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. HP has corrected this potential vulnerability. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised when a buffer overflow occurs in the CDE online help. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege. HP has corrected this potential vulnerability.
Patch 1107.00 OSF440-677	**Patch:** Fixes a problem in sys/timeb.h **State:** New This patch fixes a problem in <sys/timeb.h> where the ftime() prototype was not available in the default compilation name space.
Patch 1118.00 OSF440-983	**Patch:** Fix for grep command hang problem **State:** Supersedes patches OSF440-378 (428.00), OSF440-381 (431.00), OSF440-432 (517.00), OSF440-526 (653.00) This patch corrects the following: • Corrects a problem with the fgrep command, when it is used with the -s flag all output is suppressed. • Fixes a limitation problem with the grep and fgrep commands. If the line length is too long, grep displays a “wordlist too large” error message and fgrep displays “input too long” error message. • Fixes the following two problems: – fgrep limits are too small. – fgrep displays data files verbatim if pattern_file has blank lines. • Fixes a problem in which the grep command with the -w switch does not work as documented. • The grep command will now allow blank lines in the pattern file, and does not hang when executed with the -w and -f options.
Patch 1120.00 OSF440-795	**Patch:** Security (SSRT1-40U, SSRT1-41U, SSRT1-42U, SSRT1-45U) **State:** New This patch adds the mktemp(1) reference page for the mktemp command.

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

Patch 1122.00 OSF440X11-048A	**Patch:** Fixes a problem with PowerStorm 4D20 card **State:** New This patch fixes a problem with a Compaq Professional Workstation XP1000 667 MHz system with a PowerStorm 4D20 (PBXGB-CA) graphics card where fonts were sometimes drawn incorrectly.
Patch 1124.00 OSF440-798	**Patch:** Updates for mktemp(3) reference page **State:** New This patch updates the mktemp(3) reference page with changed information regarding the mktemp() and mkstemp() routines, and adds information about the mkdtemp() and mkstemps() libc routines.
Patch 1126.00 OSF440-927	**Patch:** Corrects improper file or privilege management **State:** Supersedes patch OSF440-211 (260.00) This patch corrects the following: • This patch fixes a problem of not completing mailsetup if the hostname ends with 0 (zero). The error message produced is: Error creating /var/adm/sendmail/.cf: exiting • 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. HP has corrected this potential vulnerability.
Patch 1128.00 OSF440X11-056	**Patch:** Various fixes for X font server **State:** Supersedes patch OSF440X11-025A (355.00) This patch corrects the following: • Fixes various problems with the X font server and with the X server's interaction with X font servers. • Fixes a problem where the X server can grow excessively when accessing certain fonts.
Patch 1130.00 OSF440DX-031	**Patch:** Corrects improper file access **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 access. HP has corrected this potential vulnerability.
Patch 1132.00 OSF440-864	**Patch:** Security (SSRT2208) **State:** New A potential security vulnerability has been identified in the HP Tru64 UNIX operating system which may allow non-privileged users to gain unauthorized (root) access. This may be in the form of local and remote security domain risks. This potential security vulnerability in routed has been corrected.
Patch 1134.00 OSF440-950	**Patch:** Fix for fwtmp command **State:** New Now fwtmp will not display the invalid (negative) pids when the number of decimal digits of pid value exceeds 5.

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

Patch 1137.00 OSF440-986	**Patch:** Corrects improper file or privilege management **State:** Supersedes patch OSF440-955 (1135.00) This patch corrects the following: • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. HP has corrected this potential vulnerability. • Addresses compiler warnings caused by calling function with too few arguments.
Patch 1141.00 OSF440-852	**Patch:** Security (SSRT2229) **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. HP has corrected this potential vulnerability.
Patch 1145.00 OSF440CDE-055	**Patch:** Corrects improper file access **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 access. HP has corrected this potential vulnerability.
Patch 1147.00 OSF440-935	**Patch:** Security (SSRT2339, SSRT2339) **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 access. HP has corrected this potential vulnerability.
Patch 1149.00 OSF440-872	**Patch:** Fix prevents simple lock owned panics **State:** New This fix prevents “simple lock owned” panics.
Patch 1151.00 OSF440DX-035	**Patch:** Corrects improper file access **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 access. HP has corrected this potential vulnerability.
Patch 1153.00 OSF440-909	**Patch:** Corrects improper file or privilege management **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. HP has corrected this potential vulnerability.

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

Patch 1159.00 OSF440X11-049A	**Patch:** Security (SSRT0753U, SSRT0752U) **State:** Supersedes patches OSF440X11-002A (62.00), OSF440X11-011A (218.00), OSF440X11-034A (542.00), OSF440X11-060A (1154.00), OSF440X11-045A (1155.00), OSF440X11-052 (1156.00), OSF440X11-061 (1157.00) This patch corrects the following: • Fixes a problem with Motif Drag-and-Drop where, if a parent drop site was unregistered before a child drop site, subsequently unregistering the child drop site would cause a segmentation fault. • Fixes a problem with the toggle button where, if a display is closed and reopened, then the X Server may generate an “Invalid Pixmap Error”. • Fixes various memory leaks in the Motif library (libXm) that could occur when creating and destroying Motif List, Text, and TextField widgets. • 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. HP has corrected this potential vulnerability. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of large values of ENVIRONMENT variables. HP has corrected this potential vulnerability. • Fixes a problem with Motif tear-off menus which may cause a core dump when the shell widget is destroyed. • Fixes a problem where XmGetPixmapByDepth may fail if a directory in the search path contains a large number of files. • This patch fixes a problem with the Motif ToggleButton Widget where, in some cases, it may not draw itself correctly.
Patch 1161.00 OSF440DX-040	**Patch:** Corrects buffer overflow in the dxsysinfo utility **State:** New A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised when a buffer overflow occurs in the dxsysinfo utility. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege.
Patch 1163.00 OSF440-863	**Patch:** Corrects improper file or privilege management **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. HP has corrected this potential vulnerability.
Patch 1165.00 OSF440DX-029	**Patch:** Corrects improper file access **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 access. HP has corrected this potential vulnerability.

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

Patch 1167.00 OSF440-869	**Patch:** Corrects improper file or privilege management **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. HP has corrected this potential vulnerability.
Patch 1169.00 OSF440-868	**Patch:** Corrects improper file or privilege management **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. HP has corrected this potential vulnerability.
Patch 1172.00 OSF440-1002	**Patch:** Elminates compiler warnings in ln **State:** Supersedes patch OSF440-969 (1170.00) Corrected the behavior of ln -sf, to address the issue caused when a symbolic link points to a non-existing file. This patch eliminates compiler warnings in ln.
Patch 1174.00 OSF440-797	**Patch:** Security (SSRT1-40U, SSRT1-41U, SSRT1-42U, SSRT1-45U) **State:** New This patch adds the safe_open(3) reference page for the safe_open() routine in libc.
Patch 1176.00 OSF440X11-054	**Patch:** Corrects improper file access **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 access. Hp has corrected this potential vulnerability.
Patch 1178.00 OSF440-978	**Patch:** Fix for various vdump problems **State:** Supersedes patches OSF440-048 (42.00), OSF440-237 (276.00), OSF440-404 (452.00), OSF440-089 (167.00), OSF440-338 (588.00), OSF440-547 (674.00) This patch corrects the following: • The command was slow to complete when a partial restore operation was requested. • The command failed to ignore extended attribute records for the files which were not requested for a vrestore operation. • Fixes problem with vrestore where vrestore fails to restore certain files and directories having ACLs from a compressed vdump saveset, reporting: vrestore: error setting extended attributes 22 • A previous patch caused incomplete restores. • A warning message is displayed when the path for the first file in a group of hardlinks is created without using original protection codes and property lists. • A warning message is displayed and vrestore aborts if it fails to malloc space for a property list. • A message which had been inserted at the end of the message file had the wrong message category (this could cause messaging confusion).

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

Patch 1178.00 continued	• An uninitialized variable in the code that restores property lists could cause malloc failures, memory faults, “error setting extended attributes” messages, and infinite loops using the -l option. • Corrupted property list information could cause an infinite loop. • Fixes a problem where the vdump program would dump core with the following message: nnnn Resources lost(coredump) • Fixes the following problems with the vdump command: – Fixes a problem where the vdump command will sometimes store symbolic link files as directories in the vdump archive. – 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. – Fixes the vdump to pickup correct messages in all locales. – Avoids some unnecessary function calls and thus allows faster vdumps. • Fixes the following problems with the vrestore command: – 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 a directory for the second occurrence of the file with the same inode number). – The -Q option is added to vrestore to allow the user to request that vrestore ignore the quota files (thus avoiding the time it takes to process them). – Fixes vrestore to pick up correct messages in all locales. – Fixes to display bit file attributes upon -l option.
Patch 1180.00 OSF440-862	**Patch:** Corrects improper file or privilege management **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. HP has corrected this potential vulnerability.

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

Patch 1182.00 OSF440X11-047A	**Patch:** Static library fix (libXt) **State:** Supersedes patches OSF440X11-005B (206.00), OSF440X11-018B (336.00), OSF440X11-033A (553.00) This patch corrects the following: • Fixes various Minor System Faults (MSFs) in the X Toolkit library (libXt). • Fixes a memory leak in the X Toolkit library (libXt). This memory leak could be seen by applications that create and destroy many Motif ScrolledWindow widgets • Fixes a memory leak in the X Window System's X Toolkit library (Xt) that could occur when creating and destroying Motif List, Text, and TextField widgets. • Fixes a problem in the X Toolkit library (Xt) which could cause the TeMIP Iconic_map Presentation Module application (mcc_iconic_map) to crash.
Patch 1184.00 OSF440-890	**Patch:** Security (SSRT0792U) **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. HP has corrected this potential vulnerability.
Patch 1186.00 OSF440-979	**Patch:** Compiler warnings addressing outside array bounds **State:** New This patch removes compiler warnings addressing outside of array bounds.
Patch 1189.00 OSF440-675	**Patch:** snmp getnext returns value of wrongOID **State:** Supersedes patches OSF440-499 (678.00), OSF440-960 (1187.00) This patch corrects the following: • Fixes a problem where os_mibs would core dump. • Fixes a problem in os_mibs which resulted in the swap size and swap used values for the host mib being reported as negative values on some systems. • Fixes the problem where snmp getnext returns back the value of the wrongOID on queries in the FDDI MIB of os_mibs.
Patch 1193.00 OSF440-848	**Patch:** Fix for restore command **State:** Supersedes patches OSF440-387 (437.00), OSF440-970 (1190.00), OSF440-1013 (1191.00) This patch corrects the following: • Fixes a problem in which the restore command can fail with the following error: Cannot malloc space for property list • Introduced dumprmt.msg for remote dump/restore messages. This new message catalog file is used in both rdump and rrestore programs. • Fixed dump to recognize LSM volumes correctly and not report random information when an error has occurred. • Eliminates the /sbin/restore program's ignoring of property lists.

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

Patch 1195.00 OSF440DX-034	**Patch:** Corrects improper file access **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 access. HP has corrected this potential vulnerability.
Patch 1197.00 OSF440-877A	**Patch:** Installs version V2.1-120 **State:** Supersedes patches OSF440-150A (124.00), OSF440-548A (680.00) This patch corrects the following: • Fixes the following problem in the libots3 run-time library: – The failure to check the return status after certain system calls caused a problem in the libots3 run-time library. The libots3 run-time library supports OpenMP parallel applications. • Fixes the following problem in the parallel processing support library (libots3): – A problem in the parallel processing support library that caused incorrect run-time results for an OpenMP program. • Installs version V2.1-120 of /usr/lib/libots3.a and /usr/shlib/libots3.so. V2.1-120 fixes a problem where long running OpenMP applications might overflow an internal libots3 counter, resulting in a breakdown of thread synchronization.
Patch 1199.00 OSF440-877B	**Patch:** Installs version V2.1-120 **State:** Supersedes patches OSF440-150B (204.00), OSF440-548B (682.00) This patch corrects the following: • Fixes the following problem in the libots3 run-time library: – The failure to check the return status after certain system calls caused a problem in the libots3 run-time library. The libots3 run-time library supports OpenMP parallel applications. • Fixes the following problem in the parallel processing support library (libots3): – A problem in the parallel processing support library that caused incorrect run-time results for an OpenMP program. • Installs version V2.1-120 of /usr/lib/libots3.a and /usr/shlib/libots3.so. V2.1-120 fixes a problem where long running OpenMP applications might overflow an internal libots3 counter, resulting in a breakdown of thread synchronization.
Patch 1202.00 OSF440CDE-040	**Patch:** Corrects improper file access **State:** Supersedes patches OSF440CDE-026 (596.00), OSF440CDE-041 (1200.00) This patch corrects the following: • Fixes a problem in which the Window Manager (dtwm) intermittently hangs on a system which uses multiple displays. • 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 access. HP has corrected this potential vulnerability. • Fixes a problem in the Window Manager (dtwm) where double-click actions are performed on the second button press instead of the second button release. This causes the second button release event to be sent to any underlying window.

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

Patch 1205.00 OSF440-710	**Patch:** NetRAIN does not failover to a backup interface **State:** Supersedes patches OSF440-267 (302.00), OSF440-638 (813.00), OSF440-592 (1203.00) This patch corrects the following: • Fixes a NetRAIN problem when using HE155 (FORE) ATM cards. NetRAIN will fail when configuring LANE to join Elans. • Fixes a problem in NetRAIN. NetRAIN interface creation now fails if any of the requested standby interfaces do not exist. • Fixes a problem with NetRAIN when switching to the standby interface. The error message is “ifconfig: ioctl (SIOCIFSWITCH): Invalid argument”. • Fixes a problem with NetRAIN which prevents it from failing over to a backup interface if the primary interface is disconnected at boot time.
Patch 1208.00 OSF440DX-026	**Patch:** Security (SSRT0785U) **State:** Supersedes patches OSF440DX-004 (189.00), OSF440DX-005 (190.00), OSF440DX-006 (191.00), OSF440DX-008 (193.00), OSF440DX-010 (214.00), OSF440DX-014 (345.00), OSF440DX-015 (346.00), OSF440DX-016 (347.00), OSF440DX-017 (348.00), OSF440DX-018 (349.00), OSF440DX-019 (559.00), OSF440DX-027 (1206.00) This patch corrects the following: • Fixes two situations in which the GUI account management program (dxaccounts) will crash in a Enhanced Security client environment when attempting to copy an NIS user account. • Fixes the problem with the useradd, usermod, and userdel commands removing the last entry of the /etc/passwd file when the last line of the /etc/passwd file does not end with the new line character (\n). • Fixes a problem where usermod -D can coredump if an NIS group entry contains a large number of users. • Fixes a problem in which the command usermod was not allowing any commas in the comment field when the current GECOS fields are filled. • Fixes a problem in which a duplicate user identifier (UID) is accepted at a second attempt even if the no-duplicate-user-identifier policy is set. • Updates the error message displayed when Account Manager fails to start due to the detection of an Account Manager lock file (/etc/.AM_is_running) on the system. • Fixes the problem in which a command usermod -D does not display the Expire date when it is set. • Fixes a problem in which dxaccounts does not allow the system manager to add NIS users when the system is running enhanced security. • Fixes the problem of enabling the change root’s login/uid through cli/dxaccounts utilities. • Fixes a problem in which the dxaccounts application does not allow users to be added to groups with Group ID lower than the default minimum specified in the General Options dialog.

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

Patch 1208.00 continued	• 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. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of passwords that have a length outside of the intended range. HP has corrected this potential vulnerability. • Fixes the problem that causes the dxaccounts application to core dump when /etc/shells is a directory instead of a file.
Patch 1211.00 OSF440-765A	**Patch:** Support for NEW_OPEN_MAX_SYSTEM in libaio **State:** Supersedes patch OSF440-793A (1209.00) This patch corrects the following: • Prevents thread blocking forever when both libaio and libaio_raw are linked into the same image. • Closes an aio_read()/aio_cancel() race condition. • Adds support for NEW_OPEN_MAX_SYSTEM (64K) file descriptors to libaio.
Patch 1214.00 OSF440-765B	**Patch:** Support for NEW_OPEN_MAX_SYSTEM in libaio **State:** Supersedes patch OSF440-793B (1212.00) This patch corrects the following: • Prevent thread blocking forever when both libaio and libaio_raw are linked into the same image. • Close an aio_read()/aio_cancel() race condition. • Adds support for NEW_OPEN_MAX_SYSTEM (64K) file descriptors to libaio.
Patch 1216.00 OSF440-910	**Patch:** Increase for ReadyTimeSeconds in ddr_config **State:** Supersedes patch OSF440-103 (80.00) This patch corrects the following: • Fixes a problem with the cdfs file system. The default a partitions are being made incorrectly by the disk driver for ISO-9660 CDs causing data corruption when reading beyond the end of a partition. Only new and non-HP CD-ROM drives are affected. • Fixes the problem where /sbin/ddr_config does not accept values for ReadyTimeSeconds larger than 255. The new limit is 86400 seconds (24 hours).
Patch 1218.00 OSF440-971	**Patch:** Corrected exit status of sed when disk is full **State:** New Corrects the exit status of sed when the disk is full.
Patch 1220.00 OSF440-930	**Patch:** Corrects improper file or privilege management **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. HP has corrected this potential vulnerability.
Patch 1226.00 OSF440-736	**Patch:** Fix for od command hang **State:** New This patch fixes a problem in which an invalid character sequence causes the od command to hang or display a partial character.

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

Patch 1228.00 OSF440-918	**Patch:** Corrects improper file or privilege management **State:** Supersedes patch OSF440-047A (41.00) This patch corrects the following: • Fixes a Y2K problem with the nroff text formatter in which the years after 1999 are translated to be 19xxx with xxx being the number of years that have passed since 1900. In this case, the year 2010 displays as 19110. • 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. HP has corrected this potential vulnerability.
Patch 1231.00 OSF440CDE-036	**Patch:** Security (SSRT1-40U, SSRT1-41U, SSRT1-42U, SSRT1-45U) **State:** Supersedes patch OSF440CDE-033 (1229.00) This patch corrects the following: • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. HP has corrected this potential vulnerability. • 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 access. HP has corrected this potential vulnerability.
Patch 1233.00 OSF440-998	**Patch:** Corrects mkdir -p functionality and eliminates mkdir compiler warnings **State:** Supersedes patch OSF440-034 (32.00) This patch corrects the following: • Fixes a problem with the mkdir -p command. The mkdir -p command did not return an error if the last component in the pathname already existed. • Eliminates compiler warnings in mkdir.
Patch 1235.00 OSF440-954	**Patch:** Corrects improper file or privilege management **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. HP has corrected this potential vulnerability.
Patch 1237.00 OSF440-878	**Patch:** Corrects a problem in the sysconfig command **State:** New This patch fixes a problem in which the lines in the output stream from sysconfig -Q can be truncated.

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

Patch 1241.00 OSF440CDE-060	**Patch:** Corrects improper file or privilege management **State:** Supersedes patches OSF440CDE-058 (1238.00), OSF440CDE-061 (1239.00) This patch corrects the following: • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. HP has corrected this potential vulnerability. • Fixes the message catalog for the CDE application dtprintinfo. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper privilege management. HP has corrected this potential vulnerability.
Patch 1244.00 OSF440-993	**Patch:** Security (SSRT0743U, SSRT2256) **State:** Supersedes patches OSF440-631 (819.00), OSF440-823 (1242.00) This patch corrects the following: • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. HP has corrected this potential vulnerability. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised when a buffer overflow occurs in the ps utility. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege. HP has corrected this potential vulnerability. • Allows whitespace in the header field with the ps -o command. Multiple headers with whitespace can be used with the ps -o command.
Patch 1246.00 OSF440-908	**Patch:** Corrects improper file or privilege management **State:** Supersedes patches OSF440-051 (45.00), OSF440-283 (316.00), OSF440-396 (444.00), OSF440-622 (821.00) This patch corrects the following: • Fixes a problem in which sort -i a_file >b_file aborts with the message “A line of the input file contains more than 20480 characters” when LANG = da_DK.ISO8859-1. • Fixes a problem in which the sort command aborts with the message “A line of the input file contains more than 20480 characters” when running in a Japanese locale. • Fixes a problem that sometimes occurs when sorting large data files in multibyte locales such as Japanese. • Corrects the behavior of the sort(1) command which now checks for duplicates with the -c, -u, and -k flags. • 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. HP has corrected this potential vulnerability. • Addresses the problem wherein performing a sort on a large database using numerous keys fails during the consolidation phase of the temporary files.

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

Patch 1248.00 OSF440-744	**Patch:** Corrects a problem with script program hang **State:** New This fix corrects a problem in which a script would hang upon exiting in a dfs configuration.
Patch 1250.00 OSF440-926	**Patch:** Corrects improper file or privilege management **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. HP has corrected this potential vulnerability.
Patch 1253.00 OSF440X11-057A	**Patch:** Security (SSRT2280) **State:** Supersedes patches OSF440X11-010A (217.00), OSF440X11-013 (219.00), OSF440X11-024 (354.00), OSF440X11-026A (356.00), OSF440X11-032A (579.00), OSF440X11-039 (711.00), OSF440X11-055A (1251.00) This patch corrects the following: • Fixes a problem in which ^C fails to work in dtterm when logged in to a 4.0E or 4.0F system using XDMCP. • Fixes a character input problem for non-Latin-1 keyboards. • Fixes a problem in which some 8-bit characters cannot be entered directly from the keyboard when the Caps Lock setting is on. • Prevents a potential core dump from the X11 library when running an input method server for Japanese, Chinese, or Korean. • 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. • This patch fixes a memory leak in the libVX11 library used by X applications where freeing a GC would not free all its memory. This problem is most likely to occur on systems with a Catetes graphics card (4D40T, 4D50T, 4D60T, or 4D51T). • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised when a buffer overflow occurs in X11 applications. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege. HP has corrected this potential vulnerability.
Patch 1255.00 OSF440-828	**Patch:** Miscellaneous linker fixes **State:** Supersedes patches OSF440-139 (113.00), OSF440-230 (207.00), OSF440-231 (208.00), OSF440-195 (249.00), OSF440-350 (401.00), OSF440-376 (580.00), OSF440-475 (582.00), OSF440-616 (691.00), OSF440-527 (692.00), OSF440-539 (693.00), OSF440-533 (695.00), OSF440-604 (825.00) This patch corrects the following: • Fixes a problem where the linker (ld) would insert incorrect values for the symbols etext and _etext when building kernels larger than 4 MB. • This patch supports the NHD2 (New Hardware Delivery Two) release. The NHD2 installation process modifies the system's linker and the osf_boot file. This patch preserves the modifications that NHD2 makes to the linker and the osf_boot file.

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

Patch 1255.00 continued	• Fixes a problem where the linker (ld) could not read arguments longer than 1024 characters in input files, and adds proper support for line continuation characters. • Addresses the failure of osf_boot to link in foreign kits with the following message: osf_boot: Not enough space to add '......... messages • Fixes a linker problem where including a shared library on a link line twice with another library in between caused unresolved symbols in some cases. • Fixes a problem in which the bootlink can fail on AlphaStations 600, 600A, and 500/400. • Fixes a potential optimization problem with the linker (/bin/ld). • Fixes two errors that occur when using the -f switch with the linker (ld): – Using the -f switch produces link errors. – Any unsupported switch beginning with -f gets interpreted to mean -f. • Fixes a problem where the linker-defined symbol _fpdata would end up being undefined if it was referenced by a program but was not used by the linker. • Fixes two problems in the linker where it would erronously report "multiply defined symbol" errors or "unresolved symbol" errors: – Modifies the linker's symbol resolution to enable it to recognize when a reference to a symbol defined in a shared library is replaced by a symbol defined in an object file or archive. – Modifies the linker to cause it to re-scan shared libraries before reporting unresolved symbols. • The .text symbol was being set incorrectly for -shared and -call_shared links. • Five linker-defined symbols were not getting the correct type set in the Dynamic Symbol Table. • This patch fixes a linker problem that may cause executables to fail with a segmentation violation when the address of an uninitialized data symbol in a shared library is used as the initial value of a global or static pointer variable.
Patch 1257.00 OSF440-845	**Patch:** Resolves KMF in DLI interrupt handler **State:** Supersedes patch OSF440-260 (295.00) This patch corrects the following: • Fixes an unaligned access panic in dli_input. • Resolves kernel memory faults in the DLI interrupt handler.
Patch 1259.00 OSF440X11-050	**Patch:** Fixes a problem in the mwm Window Manager **State:** New This patch fixes a problem in the mwm Window Manager where double-click actions are performed on the second button press instead of the second button release. This causes the second button release event to be sent to any underlying window.

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

Patch 1263.00 OSF440DX-033	**Patch:** Corrects buffer overflow occurs in the dxterm utility **State:** Supersedes patches OSF440DX-038 (1260.00), OSF440DX-032 (1261.00) A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised when a buffer overflow occurs in the dxterm utility. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege. HP has corrected this potential vulnerability.
Patch 1265.00 OSF440-796	**Patch:** Provides dirclean(8) reference page **State:** New This patch adds the dirclean(8) reference page for the /usr/sbin/dirclean utility.
Patch 1267.00 OSF440-683	**Patch:** Fixes vmstat formatting problem **State:** New In some cases, the entries in the tabular output of vmstat are improperly formatted, causing adjacent text fields to run together.
Patch 1269.00 OSF440-982	**Patch:** Fixes problems in accounting commands **State:** New This patch corrects the following problems found in accounting commands: • Resolves the differences in the CPU time and connect time, found during the conversion from ASCII format to binary format and binary format to ASCII format of accounting reports. • Resolves the differences in CPU time, found in the output of acctcom and acctmerg commands for the same input file.
Patch 1271.00 OSF440-996	**Patch:** Fix for which command **State:** New This patch fixes the which command to use the path information from the environment, rather than from the ~/.cshrc file, if it is invoked from other than the C shell.
Patch 1273.00 OSF440-994	**Patch:** Corrects improper file or privilege management **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. HP has corrected this potential vulnerability.
Patch 1275.00 OSF440-822	**Patch:** Corrects buffer overflow in binmail utility **State:** Supersedes patch OSF440-046 (40.00) This patch corrects the following: • Fixes binmail to prevent partial delivery of mail messages when disk quota is reached. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised when a buffer overflow occurs in the binmail (also called mail) utility. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege. HP has corrected this potential vulnerability.

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

Patch 1277.00 OSF440CDE-044	**Patch:** Corrects improper file access **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 access. HP has corrected this potential vulnerability.
Patch 1281.00 OSF440-825	**Patch:** Corrects improper file or privilege management **State:** Supersedes patches OSF440-932 (1278.00), OSF440-937 (1279.00) 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. HP has corrected this potential vulnerability.
Patch 1284.00 OSF440-717	**Patch:** Security (SSRT0795U) **State:** Supersedes patches OSF440-080 (159.00), OSF440-545 (699.00), OSF440-782 (1282.00) This patch corrects the following: • Fixes a problem in which a system can hang when inetd tries to start a daemon listed in inetd.conf which is not installed on the system. This can occur when a user attempts to telnet to the port reserved for the nonexistent daemon. • Corrects a problem with inetd which could result in its termination without notice and without a core file. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form where inetd may block incoming connections when scanned by nmap or other port scanners. HP has corrected this potential vulnerability. • Allows the socket listen backlog in inetd(8) to be set by using the -l option on the command line.
Patch 1286.00 OSF440-961	**Patch:** Corrects improper file or privilege management **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. HP has corrected this potential vulnerability.
Patch 1288.00 OSF440-977	**Patch:** make command now correctly checks dependencies **State:** New The make command now checks dependencies on archive libraries properly.
Patch 1290.00 OSF440CDE-031B	**Patch:** Security (SSRT0571U, SSRT0753U, SSRT0752U) **State:** Supersedes patches OSF440CDE-001 (1.00), OSF440CDE-002 (2.00), OSF440CDE-023 (528.00) This patch corrects the following: • A potential security vulnerability has been discovered where, under certain circumstances, users may gain unauthorized access. HP has corrected this potential vulnerability. • Fixes a problem where the CDE mail interface (dtmail) does not display the date and time of mail messages in the Message Header list when the time zone is set to certain time zones such as GB-Eire.

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

Patch 1290.00 continued	• 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. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of large values of ENVIRONMENT variables and command line arguments. HP has corrected this potential vulnerability.
Patch 1294.00 OSF440-981	**Patch:** Correction for merging the .login file **State:** New In a rolling upgrade, the merge of the .login file failed and did not display a message warning that it failed. This has been corrected.
Patch 1296.00 OSF440DX-039	**Patch:** Corrects improper file access **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 access. HP has corrected this potential vulnerability.
Patch 1301.00 OSF440-706	**Patch:** Fixes binlogd core dump problem **State:** OSF440-566 (703.00), OSF440-904 (1297.00), OSF440-807 (1298.00), OSF440-775 (1299.00) This patch corrects the following: • Fixes a problem in binlogd which overwrites adjacent header fields in an error record if the system's hostname is longer than 12 characters. • Fixes a problem that may prevent a correct configuration table entry from being written to the binary error log on some systems. • Causes the binary error log daemon (binlogd) to synchronize its log files before closing them upon system shutdown. • Fixes a time formatting problem when Compaq Analyze is used to display events in time zones with a positive offset from GMT. • Fixes a problem in which the binlog daemon can coredump if it attempts to recover events from a panic dump file containing invalid event data.
Patch 1303.00 OSF440-959	**Patch:** Corrects improper file or privilege management **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. HP has corrected this potential vulnerability.
Patch 1305.00 OSF440-953	**Patch:** Corrects improper file or privilege management **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. HP has corrected this potential vulnerability.
Patch 1307.00 OSF440DX-024	**Patch:** Fixes a problem in dxproctuner **State:** New This patch fixes a problem in dxproctuner where the process information is not displayed when there is a double quote followed by any other character in the command column.

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

Patch 1309.00 OSF440-928	**Patch:** Corrects improper file or privilege management **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. HP has corrected this potential vulnerability.
Patch 1312.00 OSF440-842	**Patch:** find -ls displays incorrect number of blocks **State:** Supersedes patches OSF440-384 (434.00), OSF440-988 (1310.00) This patch corrects the following: • Fixes a problem with the find command. The find command fails to show file names that start with a period. • Corrects the find -ctime, -atime, and -mtime behavior with respect to the + operations. Find + operations will match “Greater Than” rather than “Greater Than or Equal To”. • Corrects find -ls, which displayed an incorrect number of blocks.
Patch 1314.00 OSF440-888	**Patch:** Corrects improper file access **State:** Supersedes patch OSF440-277 (311.00) This patch corrects the following: • Fixes a problem in which sysconfigdb would incorrectly add or delete blank lines to or from the target file. • 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 access. HP has corrected this potential vulnerability.
Patch 1316.00 OSF440-768	**Patch:** Fix for salvage utility **State:** Supersedes patch OSF440-433 (555.00) This patch corrects several known problems with salvage: • Fixes two infinite loops that could make salvage run forever. • Salvage could core dump when encountering a deleted property list. • Removes garbage characters from symlink recovery in salvage. • Fixes a problem with the salvage utility which could cause the utility to core dump.
Patch 1318.00 OSF440-739	**Patch:** Fix for startslip program **State:** New This patch fixes a problem where startslip was not able to extract all the information from the acucap file.
Patch 1320.00 OSF440-1044A	**Patch:** Security (SSRT2400) **State:** New This patch corrects the following: • A potential security vulnerability has been discovered, where under certain circumstanes, system integrity may be compromised. HP has corrected this potential vulnerability. • Updates BIND from V4.9.3 to V8.3.4.

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

Patch 1323.00 OSF440-1044B	**Patch:** Security (SSRT2408, SSRT2410, SSRT2411) **State:** Supersedes patches OSF440-019 (17.00), OSF440-329 (383.00), OSF440-444 (534.00), OSF440-467 (661.00), OSF440-613 (794.00), OSF440-1000 (1321.00) This patch corrects the following: • Fixes a problem in which a BIND server may find that named will place a warning message in the daemon.log that was not previously seen. • Fixes a problem in which a BIND server writes files to the /etc/namedb directory instead of the /var/tmp directory. • 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. HP has corrected this potential vulnerability. • This patch fixes a problem where named could possibly core dump when printing an informational message to syslog. • Fixes a problem of named producing a core file when named is started and the named.boot file has more than 32767 zones specified. • 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. HP has corrected this potential vulnerability. • Potential BIND (Berkeley Internet Name Domain) security vulnerabilities have been reported to HP that may result in buffer overflows, unauthorized access, or denial of service (DoS) on HP Tru64 UNIX systems. These potential security vulnerabilities may be in the form of local and remote security domain risks. The following potential security vulnerabilities have been corrected: SSRT2408 BIND - (Severity - High) SSRT2410 BIND - (Severity - High) SSRT2411 BIND - (Severity - High) • A potential security vulnerability has been discovered where, under certain circumstanes, system integrity may be compromised. HP has corrected this potential vulnerability. • Updates BIND from V4.9.3 to V8.3.4.
Patch 1326.00 OSF440X11-046	**Patch:** Fix for ELSA GLoria Comet card **State:** Supersedes patches OSF440X11-004 (64.00), OSF440X11-007 (74.00), OSF440X11-009 (199.00), OSF440X11-015 (200.00), OSF440X11-016 (220.00), OSF440X11-022 (352.00), OSF440X11-029 (359.00), OSF440X11-038 (709.00), OSF440X11-059 (1324.00) This patch corrects the following: • Fixes a problem where, on systems with a Powerstorm 4D10T (ELSA GLoria Synergy) graphics board, sometimes the graphics board was not initialized properly and failed to work on power-up or when the X server was restarted. • Fixes a problem where, on systems with a Powerstorm 4D10T (ELSA GLoria Synergy) graphics board, sometimes the X server does not draw lines correctly.

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

Patch 1326.00 continued	• Provides the X server support for the PCI To Ethernet/Graphics Combo Adapter (3X-DEPVD-AA), also known as the ITI6021E Fast Ethernet NIC 3D Video Combination Adapter, InterServer Combo, or JIB. • Fixes a problem where, on systems with a Powerstorm 4D10T (ELSA GLoria Synergy) graphics board, sometimes the X server did not draw text correctly. • Fixes a problem where, on systems with a PowerStorm 4D10T (ELSA GLoria Synergy, SN-PBXGK-BB) graphics card 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). • Fixes a problem where, on systems with an ELSA GLoria Synergy graphics card, sometimes the X server would not draw stipple patterns correctly. • The ELSA GLoria Comet card does not correctly draw nested shaded boxes or anything similar.
Patch 1328.00 OSF440-929	**Patch:** Fixes improper file or privilege management **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. HP has corrected this potential vulnerability.
Patch 1331.00 OSF440X11-053	**Patch:** Correction to XCopyPlane **State:** Supersedes patches OSF440X11-035 (577.00), OSF440X11-041B (713.00), OSF440X11-043 (835.00), OSF440X11-044 (1329.00) This patch corrects the following: • Provides the Xserver library for the new 3DLabs Oxygen VX1 PCI graphics card. • Fixes the problem of erroneous pixels left behind when dragging CDE application manager icons on the desktop. • Fixes an Xserver crash when using GTK on systems using the Oxygen VX1 graphics card. • Window corruption on Oxygen VX1 graphics card if backing store/save unders are enabled. • On the Oxygen VX1 graphics card, this patch corrects XCopyPlane to only copy the requested bitplane rather than all bitplanes.

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

Patch 1337.00 OSF440CDE-031C	**Patch:** Security (SSRT0753U, SSRT0752U) **State:** Supersedes patches OSF440CDE-015 (213.00), OSF440CDE-027 (720.00), OSF440CDE-030 (839.00), OSF440CDE-059 (1332.00), OSF440CDE-057 (1333.00), OSF440CDE-043 (1334.00), OSF440CDE-045 (1335.00) This patch corrects the following: • Fixes a problem where when running the Common Desktop Environment (CDE) on a system with more than one graphics card and monitor (multihead), sometimes new windows were visible when the screen was locked. • Fixes a problem on multi-head systems in which the unlock display only works if the default display is screen 0. • Fixes the problem of palette files not been read from /etc/dt/palettes. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper privilege management. HP has corrected this potential vulnerability. • 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. HP has corrected this potential vulnerability. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of large values of ENVIRONMENT variables and command line arguments. HP has corrected this potential vulnerability.
Patch 1339.00 OSF440-936	**Patch:** Security (SSRT2368, SSRT2368) **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 access. HP has corrected this potential vulnerability.
Patch 1346.00 OSF440CDE-049	**Patch:** Security (SSRT2193) **State:** New A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised when a buffer overflow occurs in the mailcv utility. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege. HP has corrected this potential vulnerability.
Patch 1348.00 OSF440-1010	**Patch:** Fixes a problem with TULIP network interface cards **State:** Supersedes patches OSF440-345 (396.00), OSF440-647 (843.00) This patch corrects the following: • Corrects a problem with some DE500 interfaces that use the Micro Linear ML6694F PHY. • Fixes a problem with the 400ms delay upon network cable reinsertion which could lead to temporarily held drivers. • Resolves a problem where some de50x network interface cards, under specific circumstances, may not send gratuitous arp packets .

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

Patch 1356.00 OSF440CDE-022B	**Patch:** Security (SSRT0617U, SSRT0788U, SSRT0753U, SSRT0752U) **State:** Supersedes patch OSF440CDE-019B (465.00), OSF440CDE-020B (467.00), OSF440CDE-022B (586.00), OSF440CDE-034B (1349.00), OSF440CDE-042B (1350.00), OSF440CDE-056B (1351.00), OSF440CDE-048B (1352.00), OSF440CDE-039B (1353.00), OSF440CDE-037B (1354.00) This patch corrects the following: • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. HP has corrected this potential vulnerability. • Fixes a problem in which dtfile ICDE COSE tool does not work when TMPDIR is defined as /ldata/disk_local/tmp. dtfile returns this error: /ldata/disk_local/tmp/sdtdbcache_AAAaadmma: Cross-device link /ldata/disk_local/tmp/sdtdbcache_BAAaadmma: Cross-device link Floating exception (core dumped) • Fixes a problem with the Common Desktop Environment (CDE) in which some desktop applications will fail if CDE is not initialized. The error which appears in the users home .dt/errorlog file is: Desktop Not Initialized: Could not createAction/Datatypes database. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of large values of command line arguments. HP has corrected this potential vulnerability. • 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 access. HP has corrected this potential vulnerability. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised when a buffer overflow occurs in the DtSvc utility. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege. • Fixes the dtprintinfo memory fault problem with long LANG value. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of large values of ENVIRONMENT variables and command line arguments. HP has corrected this potential vulnerability.
Patch 1358.00 OSF440X11-051	**Patch:** Corrects improper file access **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 access. HP has corrected this potential vulnerability.

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

Patch 1361.00 OSF440CDE-051	**Patch:** Security (SSRT2280) **State:** Supersedes patch OSF440CDE-052 (1359.00) A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised when a buffer overflow occurs in the dtterm utility. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege. HP has corrected this potential vulnerability.
Patch 1363.00 OSF440-921	**Patch:** Corrects improper file or privilege management **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. HP has corrected this potential vulnerability.
Patch 1365.00 OSF440DX-036	**Patch:** Corrects improper file access **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 access. HP has corrected this potential vulnerability.
Patch 1368.00 OSF440-894	**Patch:** Fixes a problem in procfs **State:** Supersedes patches OSF440-321 (378.00), OSF440-556 (721.00), OSF440-576 (723.00), OSF440-589 (841.00), OSF440-824 (1366.00) This patch corrects the following: • Fixes a kernel memory fault in procfs_get_s5_dir. • Corrects a problem where attaching to a program with a debugger will cause periodic timers to be lost and will make the program hang. • Resolves problems encontered with the Ladebug and TotalView debuggers. • Fixes a problem that made setuid programs unable to open themselves. • Fixes VM locking problem in procfs. Fixes a kernel memory fault related to ioctl PIOCMAP. • Fixes a problem in procfs that, in some situations, prevents exiting threads from exiting. This creates a situation where these threads simply spin, consuming CPU time.
Patch 1370.00 OSF440-919	**Patch:** Corrects improper file or privilege management **State:** New This patch corrects the following: • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. HP has corrected this potential vulnerability. • Addresses the problem of coredump when output of lint for a non-existing file is supplied to error.

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

Patch 1372.00 OSF440-859	**Patch:** Security (SSRT0642U) **State:** Supersedes patches OSF440-149A (123.00), OSF440-251A (287.00), OSF440-301A (364.00), OSF440-370A (421.00), OSF440-462A (562.00), OSF440-439A (564.00) This patch corrects the following: • Fixes a problem of libsecurity producing a core file when handling error conditions. • 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. HP has corrected this potential vulnerability. • Corrects a problem of the rsh command displaying a warning message instead of the rsh command output when C2 security is configured. • Fixes a problem with logins in a DCE/C2 environment. The user could encounter an error “Bad priority setting” if there is a u_priority setting used in /etc/auth/system/default file. • 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 when a system is configured with DECnet, C2, and NIS. When invoking edauth(8), the error “Must be on NIS master server to update entry for <user_name>” is returned. • Corrects the problem of an incorrectly installed signal handler when Enhanced Security is enabled.
Patch 1374.00 OSF440-774	**Patch:** Security (SSRT0779U) **State:** New A potential security vulnerability has been discovered where, under certain circumstances, SNMP services can stop functioning.
Patch 1378.00 OSF440X11-049B	**Patch:** Security (SSRT0753U, SSRT0752U) **State:** Supersedes patches OSF440X11-002B (70.00), OSF440X11-011B (335.00), OSF440X11-034B (569.00), OSF440X11-060B (1375.00), OSF440X11-045B (1376.00) This patch corrects the following: • Fixes a problem with Motif Drag-and-Drop where, if a parent drop site was unregistered before a child drop site, subsequently unregistering the child drop site would cause a segmentation fault. • Fixes a problem with the toggle button where, if a display is closed and reopened, then the X Server may generate an “Invalid Pixmap Error”. • Fixes various memory leaks in the Motif library (libXm) that could occur when creating and destroying Motif List, Text, and TextField widgets. • 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. HP has corrected this potential vulnerability. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of large values of ENVIRONMENT variables. HP has corrected this potential vulnerability. • Fixes a problem with the Motif ToggleButton Widget where, in some cases, it may not draw itself correctly.

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

Patch 1380.00 OSF440-920	**Patch:** Corrects improper file or privilege management **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. HP has corrected this potential vulnerability.
Patch 1382.00 OSF440-995	**Patch:** cut command now handles incomplete lines correctly **State:** New This patch fixes the cut command to handle incomplete lines correctly.
Patch 1384.00 OSF440-820	**Patch:** Corrects improper file or privilege management **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. HP has corrected this potential vulnerability.
Patch 1386.00 OSF440DX-030	**Patch:** Corrects improper file access **State:** Supersedes patches OSF440DX-007 (192.00), OSF440DX-002 (187.00), OSF440DX-020 (571.00) This patch corrects the following: • Fixes a problem with the diskconfig utility where ri type disks were not correctly recognized. • Fixes a problem where, when creating an AdvFS partition, the disk configuration utility (/usr/sbin/diskconfig) failed with the error: Error in Tcl Script Error: can’t read dskdir: no such variable • Fixes a problem that was causing diskconfig to issue the error message “can’t read tminor: no such variable” upon startup. • 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 access. HP has corrected this potential vulnerability.
Patch 1388.00 OSF440-938	**Patch:** Fixes an IDE/ATA bus hang **State:** Supersedes patch OSF440-315 (373.00), OSF440-468 (573.00) This patch corrects the following: • Processes may hang due to waiting for I/O interrupts. • The SCU command set pages pcf will hang a system when ATAPI CD-ROM device is selected. • Corrects recognition problems with some models of IDE CD-ROM devices and removable disk devices during system startup. Some IDE devices may cause the system to hang or panic during startup and others may not be recognized. • Fixes an IDE/ATA bus hang caused by attempting to complete raw odd byte DMA transfers to and from IDE/ATAPI devices.

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

Patch 1391.00 OSF440CDE-032	**Patch:** Security (SSRT0767U, SSRT2251, SSRT2274, SSRT0788U) **State:** Supersedes patches OSF440CDE-019A (342.00), OSF440CDE-020A (343.00), OSF440CDE-022A (513.00), OSF440CDE-034A (1108.00), OSF440CDE-042A (1109.00), OSF440CDE-056A (1110.00), OSF440CDE-048A (1111.00), OSF440CDE-039A (1112.00), OSF440CDE-035 (1113.00), OSF440CDE-037A (1114.00), OSF440CDE-050 (1389.00), OSF440CDE-031A (1116.00) This patch corrects the following: • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. HP has corrected this potential vulnerability. • Fixes a problem in which dtfile ICDE COSE tool does not work when TMPDIR is defined as /ldata/disk_local/tmp. The dtfile command returns this error: /ldata/disk_local/tmp/sdtdbcache_AAAaadmma: Cross-device link /ldata/disk_local/tmp/sdtdbcache_BAAaadmma: Cross-device link Floating exception (core dumped) • Fixes a problem with the Common Desktop Environment (CDE) in which some desktop applications will fail if CDE is not initialized. The error that appears in the users home .dt/errorlog file is: Desktop Not Initialized: Could not createAction/Datatypes database. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of large values of command line arguments. HP has corrected this potential vulnerability. • 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 access. HP has corrected this potential vulnerability. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised when a buffer overflow occurs in the DtSvc utility. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege. • Fixes a potential security vulnerability in CDE Subprocess Control Service (dtspcd). The dtspcd has a potential buffer overflow condition which may lead to unauthorized access. HP has corrected this potential vulnerability. • Fixes the dtprintinfo memory fault problem with long LANG value. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of large values of ENVIRONMENT variables and command line arguments. HP has corrected this potential vulnerability. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. The ttdbserverd contains a potential buffer overflow that may allow unauthorized access. HP has corrected this potential vulnerability.

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

Patch 1393.00 OSF440X11-047B	**Patch:** Fixes memory leak in X Toolkit library **State:** Supersedes patches OSF440X11-005A (195.00), OSF440X11-018A (222.00), OSF440X11-033B (575.00) This patch corrects the following: • Fixes various Minor System Faults (MSFs) in the X Toolkit library (libXt). • Fixes a memory leak in the X Toolkit library (libXt). This memory leak could be seen by applications that create and destroy many Motif ScrolledWindow widgets. • Fixes a memory leak in the X Window System's X Toolkit library (Xt) that could occur when creating and destroying Motif List, Text, and TextField widgets. • Fixes a problem in the X Toolkit library (Xt) which could cause the TeMIP Iconic_map Presentation Module application (mcc_iconic_map) to crash.
Patch 1395.00 OSF440-846	**Patch:** Security (SSRT2189) **State:** New A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised when a buffer overflow occurs in the at command. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege. HP has corrected this potential vulnerability.
Patch 1397.00 OSF440-684	**Patch:** Fixes a problem with ATM signalling **State:** Supersedes patch OSF440-486 (733.00) This patch corrects the following: • Fixes a problem of ATM signalling going into "connection released" after a system reboot. • Fixes an ATM signaling problem.
Patch 1399.00 OSF440-713	**Patch:** XTI may experience a fatal error **State:** Supersedes patch OSF440-049 (43.00), OSF440-531 (731.00) This patch corrects the following: • Fixes a problem with XTI over TCP/IP when tcp_sendspace and tcp_recvspace have been decreased to 1K. When sending 4K data (using t_snd), the call is successful but no data has been sent and no message is returned. • Corrects a memory leak in the XTI socket code. • Corrects a problem in XTI which could result in a fatal error if a server was slow in responding and the client queues were backed up.
Patch 1401.00 OSF440-1009	**Patch:** Command transfer size changed to avoid kernel memory fault **State:** New This patch fixes re_ioctl() cases DIODCMD and DIODCDB. It has been changed to handle a case where the command transfer size has been changed to avoid a kernel memory fault.
Patch 1403.00 OSF440X11-048B	**Patch:** PowerStorm 4D20 graphics card draws fonts incorrectly **State:** New This patch fixes a problem with a Compaq Professional Workstation XP1000 667 MHz system with a PowerStorm 4D20 (PBXGB-CA) graphics card where fonts were sometimes drawn incorrectly.

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

Patch 1405.00 OSF440-892	**Patch:** Corrects improper file or privilege management **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. HP has corrected this potential vulnerability.
Patch 1414.00 OSF440-898	**Patch:** Provides fixes for the fixfdmn utility **State:** Procedes patches OSF440-619 (847.00), OSF440-759 (1406.00), OSF440-767 (1407.00), OSF440-764 (1408.00), OSF440-805 (1409.00), OSF440-1008 (1410.00), OSF440-753 (1411.00), OSF440-711 (1412.00) This patch corrects the following: • This patch provides support for the fixfdmn utility. The fixfdmn utility is a tool that is used to check and repair corrupted AdvFS domains. Refer to the operating system Release Notes for the complete description. • Fixes a case where the fixfdmn utility could core dump on a rare corruption in the tag file. • Prevents fixfdmn from changing file sizes unnecessarily. • Fixes a case were fixfdmn would abort when the same mcell was on the DDL more than once. Also allows fixfdmn to be run on domains which have been mounted under V5.1B and then moved back to an older version of the OS. • The fixfdmn utility will now remove full frag groups from the free frag list in the fileset frag file. • Allows fixfdmn to fix a rare corruption case in the RBMT/BMT0. • Allows fixfdmn to modify only one page of the transaction log. • Fixes a case where the fixfdmn utility exits prematurely with the message “Can’t allocate 0 bytes for group use array” and then instructs the user on how to make more memory available, although more memory is not needed.
Patch 1417.00 OSF440-916	**Patch:** Corrects security vulnerability **State:** Supersedes patches OSF440-228 (271.00), OSF440-925 (1415.00) This patch corrects the following: • Fixes a coredump problem with ftp(1) when a .netrc file contains an invalid macdef (macro definition). • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. HP has corrected this potential vulnerability. • Corrects a bug in the ftp(1) open command. The optional port argument now accepts port numbers between 32768 and 65535.
Patch 1419.00 OSF440-861	**Patch:** Corrects improper file or privilege management **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. HP has corrected this potential vulnerability.
Patch 1421.00 OSF440X11-058	**Patch:** Provides updated Russian keyboard map **State:** New This patch provides an updated keyboard map for the Russian 3R-LKQ48-BT keyboard model.

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

Patch 1423.00 OSF440-856	**Patch:** Corrects improper file or privilege management **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. HP has corrected this potential vulnerability.
Patch 1425.00 OSF440-790	**Patch:** Provides the ckfsec(1) reference page **State:** New This patch delivers the ckfsec(1) reference page.
Patch 1427.00 OSF440-956	**Patch:** Corrects improper file or privilege management **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. HP has corrected this potential vulnerability.
Patch 1429.00 OSF440-712	**Patch:** Security (SSRT0664U, SSRT0762U) **State:** Supersedes patches OSF440-178 (236.00), OSF440-524 (742.00), OSF440-494 (744.00) This patch corrects the following: • Fixes a problem that occurs when using ftp. When mget or nlist specify a filename with metacharacters and the mode is ASCII, the file is returned with <LF> as the end-of-file separator. With this patch, files are returned with <CR><LF> as the end-of-file separator. • Corrects a problem with the ftp daemon which could result in PC ftp clients hanging when transferring some files in ASCII mode. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. HP has corrected this potential vulnerability. • Corrects a problem with an ftp daemon failure when using globbing string of several asterisks. An additional correction was made for a character drop with the put command.
Patch 1431.00 OSF440-917	**Patch:** Corrects improper file or privilege management **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. HP has corrected this potential vulnerability.
Patch 1433.00 OSF440-789	**Patch:** Provides the ckfsec utility **State:** Supersedes patches A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of certain files in world-writable directories. This patch provides the ckfsec utility which can help detect such files.

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

Patch 1435.00 OSF440-761	**Patch:** Security (SSRT0794U) **State:** Supersedes patch OSF440-022 (20.00) This patch corrects the following: • Fixes a problem that prevents a user from using the ipcs command on a system whose kernel has been booted from a file that is not /vmunix. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. HP has corrected this potential vulnerability.
Patch 1437.00 OSF440-812	**Patch:** Correction for remote debugging with dbx -remote **State:** New This patch corrects a problem with remote debugging of a system kernel so that it is now possible to do so with KDEBUG enabled.
Patch 1439.00 OSF440-760	**Patch:** savecore prematurely terminates crash dump recovery **State:** New This patch corrects a problem where savecore may prematurely terminate crash dump recovery on partitions larger than 4GB.
Patch 1442.00 OSF440CDE-053B	**Patch:** Security (SSRT1-80U) **State:** Supersedes patches OSF440CDE-029B (853.00), OSF440CDE-054B (1440.00) This patch corrects the following: • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. HP has corrected this potential vulnerability. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised when a buffer overflow occurs in the CDE online help. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised when a buffer overflow occurs in the CDE online help. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege. HP has corrected this potential vulnerability.
Patch 1444.00 OSF440-857	**Patch:** Corrects improper file or privilege management **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. HP has corrected this potential vulnerability.
Patch 1446.00 OSF440-944	**Patch:** scu displays misleading data expected pattern **State:** New This patch fixes a problem with scu where a mismatch between expected and found data displays incorrect data expected.

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

Patch 1449.00 OSF440X11-057B	**Patch:** Security (SSRT2280) **State:** Supersedes patches OSF440X11-010B (334.00), OSF440X11-026B (471.00), OSF440X11-032B (594.00), OSF440X11-055B (1447.00) This patch corrects the following: • Fixes a problem in which ^C fails to work in dtterm when logged in to a 4.0E or 4.0F system using XDMCP. • Prevents a potential core dump from the X11 library when running an input method server for Japanese, Chinese, or Korean. • 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. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised when a buffer overflow occurs in X11 applications. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege. HP has corrected this potential vulnerability.
Patch 1451.00 OSF440CDE-046	**Patch:** CDE login screen truncates message in issue file **State:** New This patch fixes a problem where the CDE login screen may truncate the message contained in the /etc/issue file when it is displayed.
Patch 1456.00 OSF440-1046	**Patch:** Fixes a problem with gated **State:** New This patch fixes a core dump problem with the gated daemon.
Patch 1458.00 OSF440-1052	**Patch:** Security (SSRT3469, SSRT3531) **State:** Supersedes patches OSF440-290 (322.00), OSF440-1019 (1292.00) This patch corrects the following: • Fixes a problem where sendmail core dumped when trying to send certain 8-bit, mime-encoded files. • A potential security vulnerability has been identified in sendmail which may result in non-privileged users gaining unauthorized access to files or privileged access on the system. This potential vulnerability may be in the form of a local or remote security domain risk. • A potential security vulnerability has been reported that may result in unauthorized Privileged Access or a Denial of Service (DoS). This potential vulnerability may be in the form of local and remote security domain risks. HP has corrected this potential vulnerability. SSRT3531 sendmail - (Severity - High)

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

Patch 1464.00
OSF440-1054
	Patch: Security (SSRT2400)
	State: New
	This patch revises the following reference pages for the update of BIND from V4.9.3 to V8.3.4:
	named.boot(4)
	named.conf(4)
	named.star(4)
	resolver(4)
	bind_intro(7)
	bind_manual_setup(7)
	named-bootconf(8)
	named-xfer(8)
	named(8)
	nslookup(8)

Patch 1466.00 OSF440-1049	**Patch:** Fixes a problem in rpc.lockd **State:** Supersedes patch OSF440-496 (686.00) This patch corrects the following: • Fixes a problem in rpc.lockd where the FCNTL () function fails to lock NFS mounted directories. • Fixes three issues with rpc.lockd dealing with replies to message passing RPCs, requests from hosts with multiple IP addresses, and grant messages issued to down clients.
Patch 1468.00 OSF440-1067	**Patch:** Fixes a potential panic in the auditing of the swapctl syscall **State:** New This patch fixes a potential panic in the auditing of the swapctl syscall.
Patch 1470.00 OSF440-788C	**Patch:** Security (SSRT1-40U, SSRT1-41U, SSRT1-42U, SSRT1-45U) **State:** New A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file access. HP has corrected this potential vulnerability.
Patch 1476.00 OSF440-1037	**Patch:** Fix for rm command **State:** Supersedes patch OSF440-989 (1139.00) This patch corrects the following: • Addresses a performance issue of rm -r with large directories. • Fixes a problem with the race condition in the rm command, wherein two threads can successfully delete a file simultaneously.
Patch 1478.00 OSF440-1050	**Patch:** Security (SSRT3498, SSRT3498) **State:** New This patch fixes a potential problem in screend.
Patch 1480.00 OSF440-1043	**Patch:** Fixes SDLT media error caused bus resets **State:** Supersedes patches OSF440-062 (56.00), OSF440-119 (95.00), OSF440-129 (103.00), OSF440-072 (151.00), OSF440-235 (274.00), OSF440-386 (436.00), OSF440-561 (714.00), OSF440-568 (716.00), OSF440-601 (837.00), OSF440-780 (1340.00), OSF440-900 (1341.00), OSF440-723 (1342.00), OSF440-901 (1344.00) This patch corrects the following: • Fixes a problem in which a system with a KZPCA host bus adapter may hang when the SCSI bus is reset.

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

Patch 1480.00 continued	• Fixes excessive I/O command timeouts when using KZPCM on CLIPPERs causing disk I/O to be retried and fatal tape I/O errors. Additionally, the ITPSA driver now supports the KZPCM, 8951U, and 8952U adapters. Support has also been added to identify hardware in the event log. • Fixes the following problems related to the ITPSA driver that supports the KZPCM adapter: – A panic, machine check, or hang can occur when aborting an I/O due to a command timeout or aborting an application program with pending I/Os. – Errors can occur while the system is processing a SCSI bus or SCSI bus device reset request that is issued from the class driver. – On the 8951U and 8952U adapters, SCSI bus resets are lost when these adapters are connected to single-ended drives. – A panic can occur during boot when lockmode is set to 4. • Fixes a problem with the ITPSA driver for KZPCM and KZPCA devices which resulted in a synchronization problem, causing the SCSI bus to hang. • Fixes the following ITPSA driver problems: – The chip interrupt register fields in error log are incorrect. – Lessens the opportunity of aborts being issued for an already completed I/O. – A kernel memory fault panic caused by a SWS data structure being released twice. – A simple lock timeout panic. It was possible for a bus reset to be generated before the previous bus reset was processed, causing excessive processing within the ISR. – The driver negotiated for ULTRA2 speed when it was attached to a single-ended bus. – The system will panic in itpsa_allocReq() on boot when lockmode=4 is set. – Fixes a problem with some slower tape devices serviced by the ITPSA driver by lengthening the timeout value used. – Fixes a problem that can cause a simple lock timeout or a kernel memory fault on EV6 systems using the ITPSA driver. – Fixes a panic in the ITPSA driver. It is seen when an abort to the SCSI rewind command is issued to a TLZ10 tape device. • Adds the capability for KZPCA devices to work with SCSI devices that only support asynchronous data transfers. • Fixes a kernel memory fault related to the KZPCA adapter. • Fixes a kernel memory fault panic after an “ITPSA: itpsa_action - error converting path ID to ITPSA softc structure” message. • Fixes the SDLT media error which caused bus resets with KZPCA adapters. • Fixes a problem in the KZPCA ITPSA driver that is seen when a SCSI target presents multiple LUNs.
Patch 1482.00 OSF440-1036	**Patch:** Fixes a buffer overflow problem in the write command **State:** New This patch fixes a buffer overflow problem in the write command.

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

Patch 1491.00 OSF440-1094	**Patch:** Fix for tape read-write operations failure **State:** Supersedes patches OSF440-005 (44.00), OSF440-224 (267.00), OSF440-238 (277.00), OSF440-255 (290.00), OSF440-319 (333.00), OSF440-298 (363.00), OSF440-308 (367.00), OSF440-406 (454.00), OSF440-422 (546.00), OSF440-625 (815.00), OSF440-899 (1221.00), OSF440-745 (1222.00), OSF440-923 (1224.00), OSF440-1084 (1487.00), OSF440-100 (77.00), OSF440-248 (284.00), OSF440-624 (809.00) This patch corrects the following: • Fixes a kmf problem in bucket 2 (64-byte bucket) when the type of SCSI device dynamically changes. • Corrects a problem in which the wrong status could be returned when using a tape device. • Increases the performance of random I/O on the HSG80 disk controller. • Fixes a problem in which the system can panic with a kernel memory fault. • Fixes a problem with continuous resets when an I/O command is causing the resets. • Fixes a problem with a read capacity recovery failure. • Fixes a problem with bad block replacement (BBR) processing. • Fixes a problem where programs that read, analyze, and monitor disk statistics (such as collect) will occasionally display incorrect results. • Fixes a problem in which the system can panic with a kernel memory fault during an installation with an HSZ70 or HSZ80 connected to the system. • Fixes a problem when the type of SCSI device dynamically changes, which can result in a kernel memory fault or memory corruption panic. • Fixes a simple lock panic. • Corrects a problem where interrupting an aseagent daemon with a signal can cause devices to become unaccessible. • Fixes erroneous disk utilization values reported by the table system call. • Fixes a problem where threads are hung in I/O after a disk device has completed error recovery. • Adds support for the SuperDLT1 and the SDLT320. • Provides support for possible future tape devices. • Fixes the problem where the tapex -L command would report failure when run on certain devices. The failure would be reported when the command was run on certain TLZ09 devices, depending on the firmware. • Fixes a problem that could result in unit attention status being missed. • Fixes the problem where tape read/write operations fail with following repetitive binary.errorlog message: ctape_strategy: Device state flags indicate a Reserve is Pending • Fixes the problem where tapes reporting a SCSI version other than 2 would not work properly.

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

Patch 1493.00 OSF440-1100	**Patch:** Security (SSRT2275, SSRT2301, SSRT2309, SSRT2412) **State:** Supersedes patches OSF440-426 (532.00), OSF440-443 (515.00), OSF440-285 (318.00), OSF440-171 (231.00), OSF440-343 (394.00), OSF440-400 (448.00), OSF440-113 (89.00), OSF440-177 (235.00), OSF440-184 (241.00), OSF440-053 (47.00), OSF440-334 (387.00), OSF440-529 (701.00), OSF440-608 (833.00), OSF440-236 (275.00), OSF440-254 (289.00), OSF440-333 (386.00), OSF440-485 (538.00), OSF440-452 (540.00), OSF440-509 (666.00), OSF440-658 (807.00), OSF440-114 (90.00), OSF440-009 (168.00), OSF440-226 (269.00), OSF440-401 (449.00), OSF440-017 (15.00), OSF440-026 (23.00), OSF440-027 (24.00), OSF440-028 (25.00), OSF440-146 (120.00), OSF440-055 (142.00), OSF440-066 (145.00), OSF440-077 (156.00), OSF440-096 (175.00), OSF440-318 (376.00), OSF440-359 (410.00), OSF440-392 (440.00), OSF440-464 (521.00), OSF440-390 (654.00), OSF440-532 (655.00), OSF440-551 (656.00), OSF440-498 (657.00), OSF440-552 (659.00), OSF440-599 (790.00), OSF440-620 (792.00), OSF440-102 (79.00), OSF440-151 (125.00), OSF440-035 (138.00), OSF440-093 (172.00), OSF440-115 (91.00), OSF440-098 (177.00), OSF440-094 (173.00), OSF440-193 (247.00), OSF440-223 (266.00), OSF440-357 (408.00), OSF440-054A (48.00), OSF440-388 (438.00), OSF440-111 (87.00), OSF440-411A (457.00), OSF440-431 (508.00), OSF440-423 (509.00), OSF440-479 (511.00), OSF440-510 (647.00), OSF440-535 (648.00), OSF440-542 (649.00), OSF440-495 (651.00), OSF440-584 (786.00), OSF440-595 (787.00), OSF440-654 (789.00), OSF440-371 (422.00), OSF440-474 (549.00), OSF440-466 (551.00), OSF440-588 (811.00), OSF440-021 (135.00), OSF440-052A (46.00), OSF440-130 (104.00), OSF440-064 (144.00), OSF440-472 (557.00), OSF440-078 (72.00), OSF440-198 (251.00), OSF440-368 (419.00), OSF440-349 (400.00), OSF440-131A (105.00), OSF440-122A (98.00), OSF440-199 (252.00), OSF440-014 (12.00), OSF440-109 (85.00), OSF440-412 (458.00), OSF440-455 (544.00), OSF440-101 (78.00), OSF440-391 (439.00), OSF440-565 (688.00), OSF440-154 (128.00), OSF440-258 (293.00), OSF440-275 (309.00), OSF440-478 (522.00), OSF440-484 (524.00), OSF440-563 (662.00), OSF440-528 (664.00), OSF440-641A (797.00), OSF440-609 (799.00), OSF440-642 (831.00), OSF440-007 (59.00), OSF440-304 (330.00), OSF440-037 (139.00), OSF440-121 (97.00), OSF440-038 (140.00), OSF440-044 (39.00), OSF440-087 (165.00), OSF440-167 (228.00), OSF440-266 (301.00), OSF440-445 (590.00), OSF440-004 (34.00), OSF440-011 (9.00), OSF440-012 (10.00), OSF440-015 (13.00), OSF440-003 (27.00), OSF440-032 (30.00), OSF440-061 (55.00), OSF440-120 (96.00), OSF440-123 (99.00), OSF440-128 (102.00), OSF440-132 (106.00), OSF440-133 (107.00), OSF440-136 (110.00), OSF440-142 (116.00), OSF440-143 (117.00), OSF440-148 (122.00), OSF440-152 (126.00), OSF440-155 (129.00), OSF440-039 (141.00), OSF440-067 (146.00), OSF440-081 (160.00), OSF440-085 (164.00), OSF440-095 (174.00), OSF440-033A (31.00), OSF440-099 (178.00), OSF440-104A (81.00), OSF440-138 (112.00), OSF440-164 (134.00), OSF440-158 (224.00), OSF440-229 (272.00), OSF440-170 (230.00), OSF440-180 (238.00), OSF440-182 (239.00), OSF440-187 (244.00), OSF440-194 (248.00), OSF440-204 (255.00), OSF440-206 (257.00), OSF440-209 (259.00), OSF440-221 (265.00), OSF440-227 (270.00), OSF440-256 (291.00), OSF440-259 (294.00), OSF440-268 (303.00), OSF440-272 (307.00), OSF440-276 (310.00), OSF440-278 (312.00), OSF440-284 (317.00), OSF440-144 (118.00), OSF440-036 (33.00), OSF440-056 (49.00), OSF440-057 (50.00), OSF440-058 (51.00), OSF440-059 (52.00), OSF440-112 (88.00), OSF440-125 (100.00), OSF440-141 (115.00), OSF440-147 (121.00), OSF440-060A (54.00), OSF440-082 (161.00), OSF440-305 (331.00), OSF440-166 (227.00), OSF440-174 (234.00), OSF440-208 (258.00), OSF440-213 (261.00), OSF440-220 (264.00), OSF440-244 (280.00), OSF440-257 (292.00), OSF440-265 (300.00), OSF440-289 (321.00), OSF440-097A (176.00),

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

Patch 1493.00 continued	OSF440-303 (329.00), OSF440-168A (229.00), OSF440-107 (83.00), OSF440-191 (246.00), OSF440-159 (131.00), OSF440-088 (73.00), OSF440-065 (58.00), OSF440-207 (180.00), OSF440-239 (210.00), OSF440-253 (288.00), OSF440-269 (304.00), OSF440-288 (320.00), OSF440-294 (326.00), OSF440-018 (16.00), OSF440-157 (130.00), OSF440-314 (332.00), OSF440-073 (152.00), OSF440-219 (263.00), OSF440-116 (92.00), OSF440-070 (149.00), OSF440-071 (150.00), OSF440-216 (181.00), OSF440-196 (250.00), OSF440-240 (278.00), OSF440-270 (305.00), OSF440-110 (86.00), OSF440-292 (324.00), OSF440-160 (132.00), OSF440-200 (360.00), OSF440-297 (362.00), OSF440-302 (365.00), OSF440-307 (366.00), OSF440-309 (368.00), OSF440-310 (369.00), OSF440-311 (370.00), OSF440-312 (371.00), OSF440-313 (372.00), OSF440-317 (375.00), OSF440-320 (377.00), OSF440-322 (379.00), OSF440-324 (380.00), OSF440-328 (382.00), OSF440-335 (388.00), OSF440-337 (389.00), OSF440-340 (391.00), OSF440-341 (392.00), OSF440-342 (393.00), OSF440-346 (397.00), OSF440-347 (398.00), OSF440-348 (399.00), OSF440-352 (403.00), OSF440-353 (404.00), OSF440-360 (411.00), OSF440-361 (412.00), OSF440-362 (413.00), OSF440-363 (414.00), OSF440-367 (418.00), OSF440-372 (423.00), OSF440-373 (424.00), OSF440-374 (425.00), OSF440-375 (426.00), OSF440-379 (429.00), OSF440-380 (430.00), OSF440-382 (432.00), OSF440-383 (433.00), OSF440-393 (441.00), OSF440-394 (442.00), OSF440-397 (445.00), OSF440-398 (446.00), OSF440-405 (453.00), OSF440-407 (455.00), OSF440-414 (459.00), OSF440-415 (460.00), OSF440-417 (462.00), OSF440-295 (327.00), OSF440-250 (286.00), OSF440-331 (385.00), OSF440-419 (464.00), OSF440-418 (463.00), OSF440-364 (415.00), OSF440-408 (456.00), OSF440-135 (109.00), OSF440-140 (114.00), OSF440-225 (268.00), OSF440-263 (298.00), OSF440-434 (483.00), OSF440-424 (484.00), OSF440-436A (485.00), OSF440-457 (486.00), OSF440-480 (487.00), OSF440-458 (488.00), OSF440-447 (489.00), OSF440-483 (490.00), OSF440-450 (491.00), OSF440-481 (492.00), OSF440-435 (493.00), OSF440-454 (494.00), OSF440-427 (495.00), OSF440-456 (496.00), OSF440-477 (497.00), OSF440-449 (498.00), OSF440-471 (499.00), OSF440-442 (500.00), OSF440-482 (501.00), OSF440-446 (502.00), OSF440-465 (503.00), OSF440-469 (505.00), OSF440-063 (57.00), OSF440-075 (154.00), OSF440-476 (519.00), OSF440-534 (599.00), OSF440-578 (600.00), OSF440-579 (601.00), OSF440-514 (602.00), OSF440-559 (603.00), OSF440-554 (604.00), OSF440-550 (605.00), OSF440-492 (606.00), OSF440-489 (607.00), OSF440-567 (608.00), OSF440-605 (609.00), OSF440-544A (610.00), OSF440-574 (611.00), OSF440-530 (612.00), OSF440-500 (613.00), OSF440-490 (614.00), OSF440-577 (615.00), OSF440-540 (616.00), OSF440-585A (617.00), OSF440-569 (618.00), OSF440-546 (619.00), OSF440-497 (620.00), OSF440-503 (621.00), OSF440-505 (622.00), OSF440-522 (623.00), OSF440-487 (624.00), OSF440-562 (625.00), OSF440-460 (626.00), OSF440-560 (627.00), OSF440-570 (628.00), OSF440-558 (629.00), OSF440-553 (630.00), OSF440-543 (631.00), OSF440-536 (632.00), OSF440-491 (633.00), OSF440-557 (634.00), OSF440-617 (635.00), OSF440-525 (636.00), OSF440-501 (637.00), OSF440-504 (638.00), OSF440-549 (640.00), OSF440-656 (747.00), OSF440-632 (748.00), OSF440-651 (749.00), OSF440-630 (750.00), OSF440-629 (751.00), OSF440-612 (752.00), OSF440-636 (753.00), OSF440-590A (754.00), OSF440-665 (755.00), OSF440-655 (756.00), OSF440-633 (757.00), OSF440-646 (758.00), OSF440-635 (759.00), OSF440-600 (760.00), OSF440-649 (761.00), OSF440-593 (762.00), OSF440-645 (763.00), OSF440-652 (764.00), OSF440-626 (765.00), OSF440-653 (766.00), OSF440-611 (767.00), OSF440-597 (768.00), OSF440-648 (769.00), OSF440-657 (770.00), OSF440-634 (771.00), OSF440-644 (772.00), OSF440-573 (773.00), OSF440-628 (774.00), OSF440-621 (775.00), OSF440-603 (776.00), OSF440-660 (777.00), OSF440-666 (778.00),

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

Patch 1493.00 continued	OSF440-596 (779.00), OSF440-602 (781.00), OSF440-703 (857.00), OSF440-729 (859.00), OSF440-090 (169.00), OSF440-188 (245.00), OSF440-734 (860.00), OSF440-931 (861.00), OSF440-1015 (862.00), OSF440-792 (863.00), OSF440-972 (864.00), OSF440-897 (865.00), OSF440-803 (866.00), OSF440-778 (867.00), OSF440-682 (868.00), OSF440-887 (869.00), OSF440-873A (870.00), OSF440-913 (871.00), OSF440-671 (872.00), OSF440-670 (873.00), OSF440-678 (874.00), OSF440-817 (875.00), OSF440-1016 (876.00), OSF440-732 (877.00), OSF440-962 (878.00), OSF440-756 (879.00), OSF440-968 (880.00), OSF440-1007 (881.00), OSF440-763 (882.00), OSF440-844 (883.00), OSF440-1011 (884.00), OSF440-801 (885.00), OSF440-896 (886.00), OSF440-985 (887.00), OSF440-827 (888.00), OSF440-990 (889.00), OSF440-781 (890.00), OSF440-668 (891.00), OSF440-870 (892.00), OSF440-1018 (893.00), OSF440-811 (894.00), OSF440-924 (895.00), OSF440-693 (896.00), OSF440-847 (897.00), OSF440-849 (898.00), OSF440-769 (899.00), OSF440-837 (900.00), OSF440-700 (901.00), OSF440-911 (902.00), OSF440-720 (903.00), OSF440-934A (904.00), OSF440-941 (905.00), OSF440-725 (906.00), OSF440-779 (907.00), OSF440-709 (908.00), OSF440-1012 (909.00), OSF440-893 (910.00), OSF440-946 (911.00), OSF440-718 (912.00), OSF440-762 (913.00), OSF440-838 (914.00), OSF440-940 (915.00), OSF440-964 (916.00), OSF440-730 (917.00), OSF440-879 (918.00), OSF440-1003 (919.00), OSF440-902 (920.00), OSF440-695 (921.00), OSF440-914 (922.00), OSF440-991 (923.00), OSF440-786 (924.00), OSF440-831 (925.00), OSF440-771 (926.00), OSF440-776 (927.00), OSF440-791 (928.00), OSF440-699 (929.00), OSF440-701 (930.00), OSF440-741 (931.00), OSF440-679 (932.00), OSF440-886 (933.00), OSF440-672 (934.00), OSF440-905 (935.00), OSF440-716 (936.00), OSF440-802 (937.00), OSF440-726 (938.00), OSF440-922 (939.00), OSF440-697 (940.00), OSF440-881 (941.00), OSF440-692 (942.00), OSF440-738 (943.00), OSF440-737 (944.00), OSF440-698 (945.00), OSF440-952 (946.00), OSF440-663 (947.00), OSF440-819 (948.00), OSF440-866 (949.00), OSF440-788A (950.00), OSF440-661 (951.00), OSF440-742 (952.00), OSF440-874 (953.00), OSF440-821 (954.00), OSF440-841 (955.00), OSF440-664 (956.00), OSF440-809 (957.00), OSF440-676 (958.00), OSF440-833 (959.00), OSF440-806 (960.00), OSF440-880 (961.00), OSF440-794 (962.00), OSF440-984A (963.00), OSF440-951 (964.00), OSF440-685 (965.00), OSF440-987 (966.00), OSF440-884 (967.00), OSF440-814 (968.00), OSF440-876 (969.00), OSF440-1034 (970.00), OSF440-903 (971.00), OSF440-707 (972.00), OSF440-907 (973.00), OSF440-1001 (974.00), OSF440-799 (975.00), OSF440-757 (976.00), OSF440-1004 (977.00), OSF440-748 (978.00), OSF440-889 (979.00), OSF440-816 (980.00), OSF440-754 (981.00), OSF440-687 (982.00), OSF440-1005 (983.00), OSF440-835 (984.00), OSF440-772 (985.00), OSF440-673 (986.00), OSF440-854 (987.00), OSF440-997 (988.00), OSF440-688 (989.00), OSF440-933 (990.00), OSF440-832 (991.00), OSF440-966 (992.00), OSF440-719 (993.00), OSF440-727 (994.00), OSF440-992A (995.00), OSF440-895 (996.00), OSF440-826 (997.00), OSF440-715 (998.00), OSF440-680 (999.00), OSF440-785 (1000.00), OSF440-810A (1001.00), OSF440-834 (1002.00), OSF440-836 (1003.00), OSF440-906 (1004.00), OSF440-875 (1005.00), OSF440-714 (1006.00), OSF440-829 (1007.00), OSF440-689 (1008.00), OSF440-915 (1009.00), OSF440-818 (1010.00), OSF440-783 (1011.00), OSF440-973 (1012.00), OSF440-691 (1013.00), OSF440-702 (1014.00), OSF440-871 (1015.00), OSF440-808 (1016.00), OSF440-733 (1017.00), OSF440-843 (1018.00), OSF440-850A (1019.00), OSF440-967 (1020.00), OSF440-721 (1021.00), OSF440-787 (1022.00), OSF440-976 (1023.00), OSF440-963 (1024.00), OSF440-882 (1025.00), OSF440-957 (1026.00), OSF440-813 (1027.00), OSF440-743 (1028.00), OSF440-867 (1029.00), OSF440-815 (1030.00), OSF440-746 (1031.00),

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

Patch 1493.00 continued	OSF440-669 (1032.00), OSF440-735 (1033.00), OSF440-912 (1034.00), OSF440-749 (1035.00), OSF440-770 (1036.00), OSF440-728 (1037.00), OSF440-942 (1038.00), OSF440-667 (1039.00), OSF440-696 (1040.00), OSF440-694 (1041.00), OSF440-840 (1042.00), OSF440-724 (1043.00), OSF440-740 (1044.00), OSF440-1017 (1045.00), OSF440-758 (1046.00), OSF440-777 (1047.00), OSF440-855 (1048.00), OSF440-690 (1049.00), OSF440-662 (1050.00), OSF440-860 (1051.00), OSF440-755 (1052.00), OSF440-865 (1053.00), OSF440-830 (1054.00), OSF440-949 (1055.00), OSF440-705 (1452.00), OSF440-708 (1057.00), OSF440-965 (1143.00), OSF440-1026 (1460.00), OSF440-1048 (1454.00), OSF440-1053 (1459.00), OSF440-1065 (1461.00), OSF440-1063 (1462.00), OSF440-1070 (1471.00), OSF440-1020 (1472.00), OSF440-1024 (1474.00), OSF440-1083 (1483.00), OSF440-1076 (1485.00), OSF440–1088 (1489.00) This patch corrects the following: • Corrects slow shutdown due to name lookups while deleting routes. • Prevents a “not currently mounted” warning message from being displayed for file systems the user did not request to umount. • Fixes a problem with the btcreate command where it does not pass the full pathname to newfs. • Corrects a problem in the btextract script which could result in the failure of the script due to a problem in the use of the grep utility in the script. • Fixes a problem with the btcreate command where default restore fails if disklabel is different. • Fixes a problem with btcreate not waiting long enough for the next tape to be loaded with some media changers. • Fixes system crashes seen on ASE or TruCluster systems when changing the network interfaces. The stack is not informative and the panic may be “trap: illegal instruction”, or “kernel memory fault”. • Corrects a problem where ICMP redirect packets can modify the default route. • Fixes a problem where vi puts the server port into PASSALL MODE (where XON/XOFF is no longer effective). This creates garbage in the file. • Fixes the error handling when invalid multibyte sequences are encountered in the more, ex, and vi commands. • Fixes a problem in which the vi editor core dumps when it finds invalid syntax during a substitute operation. • Fixes the following editors to handle tags functionality using the CTRL-T key: vi edit ex view vedit • When printing jobs, a timeout can occur after five minutes which causes some large print jobs to stop, then resume printing from the beginning of the print job.

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

Patch 1493.00 continued	• When slave lpd daemons try to process jobs on the print queue, some of them can fail to obtain a lock on the lock file, and exit with an error. • Print jobs will print out twice. • A remote print job may fail to print, with the error message: lstat/open failed for dfA... no such file or directory • If a print job is printing, and the connection to the remote printer is lost, the print job does not resume printing after the connection is restored. • Sometimes, as sequence numbers wrap around from 999 to 000, job 000 gets submitted before, and prints before, job 999. • The lpstat -u output is incorrect. • When using the I18N ya option, the queue daemon filters will terminate after 32 jobs. • Under certain circumstances, print jobs are terminated when printing to certain printers that are connected to a DECserver through TCP/IP. • When lpd reads any data from the printer that has not been read, for local and remote connections, the read-backs for remote connections cause an additional 2-second time out which may cause a job-submit failure on the job-number wraparound. • Corrects a problem in which, under certain conditions, unnecessary error messages are written to the lpr.log file. • 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. • Introduces the JJ /etc/printcap parameter, which allows the user to choose either one TCP/IP connection for all jobs in the print queue (JJ=1), or a TCP/IP connection for each job in the print queue (JJ=0). It also closes a timing hole that existed when lpd was shutting down. • Fixes a problem in which lpd hangs when printing to advanced server queues (using /dev/null). • Fixes an lpd problem, a memory leak associated with the allocation of a buffer. • Corrects how the C shell handles 2-byte characters when running in the Japanese SJIS locale. • Corrects the printing of Japanese SJIS strings that are assigned to shell variables in the C shell (csh). • Fixes a problem in the C shell (csh) in which a segmentation fault will occur when the user defines an environmental variable which exceeds the 2048 character limitation. This limit has been lengthened to 8192 characters. • Fixes a C shell problem where multibyte characters may not be displayed properly inside quotes. • Fixes a problem with /usr/bin/ksh and the named-pipe (FIFO) communication that is used by applications.

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

Patch 1493.00 continued	• Corrects a problem that was causing ksh to core dump in vi editing mode. ksh was core dumping intermittently when using "." to repeat a command. • ksh does a segmentation fault and core dumps when displaying a here-document. • Fixes problems in ksh, file, tail, nawk, awk, and pax: – Unexpected logouts and terminal hangups occur when using the /bin/su command and /bin/ksh as a login shell. – The file command gives incorrect output concerning WAV audio files. – The tail command gives erroneous output when used with both the -n and -r flags. – The maximum number of fields per record was changed from 99 to 199 for the awk command. – The tar/pax program did not always read the last tape record of an archive. This caused confusion for scripts that were reading a series of archives on the no-rewind device. • Fixes a problem in ksh which required two SIGTERM signals to be sent to the process when it exec'ed. • Corrects a problem that may cause ksh to core dump when displaying a large here-document in a ksh script. • Fixes a problem that caused incorrect file dates to be restored when pax was used to copy files. The problem occurred in the following cases: – If the file was a nonempty directory. – If the file was the target of another symbolic link. • Fixes a core dump from ksh. • Fixes a problem with the Korn shell where data loss occurs when commands are piped together. • Fixes a problem in ksh in which a space after the -p switch would cause the command to fail. • Fixes a problem in ksh. When the current working directory is / and the command cd .. is entered, the following error message is displayed: ksh: ..: bad directory • Fixes a cpio hanging problem in the Japanese locales. • Fixes a problem with the tar command. Corruption occurs when restoring a file system that contains more than two hard links to a file. • 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. • Fixes a possible handling problem with multibyte character boundary conditions in ksh script processing.

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

Patch 1493.00 continued	• Corrects pax/tar/cpio to properly extract explicitly specified files. When an archive contained a file with extended attributes and a different file (occurring later in the archive) was specified to be extracted, improper buffer pointer management resulted in the following display (example uses tar): tar: /dev/nrmt0h : This doesn't look like a tar archive tar: /dev/nrmt0h : Skipping to next file... tar: Memory allocation failed for extended data while reading : Not enough space The directory option was similarly affected. In this case the information for the specified file was not reported. • Fixes a problem with the tar and pax programs. These programs incorrectly append files to an existing archive and cause the file to become corrupt. • Fixes two ksh problems that occur in multi-byte Asian locales. • 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. HP has corrected this potential vulnerability. • Fixes a problem in which /usr/bin/ksh hangs for certain scripts that contain wait(1). • Modifies the strftime() function to make the %V format specifier return the correct week. • Fixes a problem of password error messages not being displayed during installation of the security subsystem. • The routines wprintf(), swprint(), and fwprintf() do not handle the S format correctly. Instead of treating the data as logical characters, they treat data as bytes. • Fixes problems with rsh(1), rlogin(1), and rcp(1) if netgroup names are defined with uppercase letters. • Fixes a problem with portmap by allowing RPC select() timeouts to occur when interrupted by signals. • Fixes and enhances the quotacheck and fsck commands. • Fixes a problem in which the fsck utility may be unable to repair a UFS filesystem. • Fixes a problem in which ufs_fsck can get blocked while attempting to flush NFS buffers for a service that has become suspended. • Fixes a problem that was causing the csh globbing function to be extremely slow when accessing file information on NFS, AFS, or VMS™ file systems. • Increases the length of the user names for rsh and rexec to allow for NT interoperabilty. • Fixes a problem where gmtime() was erroneously setting the tzname[0] array. • Fixes problems in the DECthreads library for Tru64 UNIX. Included in this patch are changes to support Ladebug enhancements and a bug fix for applications which employ SCS threads of different priorities. • Fixes bugs in the DECthreads library that would affect threaded applications running on Tru64 UNIX V4.0F. The changes are related to synchronous signal processing and thread scheduling. • Addresses performance and scalibility issues for highly contended threaded applications running on EV6 SMP machines.

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

Patch 1493.00
continued

- Fixes a problem in libc that affects debugger tracebacks of code containing split procedures.
- Adds functionality to terminate the resulting string from calls to swprintf().
- Fixes a problem for those applications that assume initial allocations of memory from the C run-time library's malloc() function will return only zero-filled memory.
- 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. HP has corrected this potential vulnerability.
- Fixes four problems for threaded applications on Tru64 UNIX V4.0F:
  - _pthreads_legacy_init_routine shows up as an unresolved symbol.
  - Programs linked -taso experienced truncated address values resulting in SEGV or data corruption errors.
  - A memory leak when the pthread_attr_setname_np function is used.
  - pthread_setname_np occasionally returning an EINVAL error.
- Fixes a bug where quotacheck -v <filestystem> will report that it has fixed some quotas. If you keep running the command, it will keep reporting the exact same fixes.
- Fixes a problem that effects threaded programs compiled with the taso option on Tru64 UNIX V4.0F. The default stack size for taso user threads in DECthreads V3.16 was too large.
- Corrects the problem of a rexec command hanging on a system.
- Fixes the following problems with the mv command:
  - An invalid error message when attempting to move files in which the source name is the same as the destination name.
  - When using mv -i to rename a symlink pointing to a file on a different file system owned by a different user, it results in the prompt:

    Ownership of y will change. Continue?
  - When moving a file from one file system to another, the mv command will copy the file rather than using the rename() system call. This can result in file loss.
- Corrects the problem with the mv(1) command deleting files in the directory when the user moves a directory to itself.
- Fixes a problem in which the mv command will not perform a move if the inode of the file is the same as the inode of the destination directory, even though the file and directory are on different file systems.
- Eliminates the previous limitation on the maximum number of external symbols that could be handled by the ar command.
- The keymap used with curses functionality was not in sync with the table contained in the term.h header file. This change corrects that and enables several nonfunctioning keys in curses-based applications.
- Fixes a problem where systems could hang in the audit code, preventing rlogins or telnets into it.

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

Patch 1493.00 continued	• When starting or stopping NFS, NFS was not checking for NFS daemons running. • rpc.pcnfsd was causing core dumps when receiving a SIGTERM signal. • Fixes a problem with the what command. This command was unable to process more than one input file at once. • Updates the FORE ATM (lfa) driver to Revision V1.0.14. • Updates the lfa ATM driver to V1.0.16 and fixes the following two ATM driver problems: – Fixes a soft hang that can occur when running NFS over ATM. – Allows the ATM subsyst. • 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. • Fixes a problem of NetRAIN devices failing to come up after the rcinet restart command is entered. • This patch fixes a class_admin/class_daemon problem. When a PID is added to a class it cannot be removed from the class scheduler until the process terminates or the class_scheduler has been stopped. • Fixes the name demangling for the tools that print symbol table names generated by the C++ V6.2 compiler. This problem will only occur for most C++ objects compiled with the ANSI options. • Fixes a problem with nm that can cause a core dump when the LANG environment variable is set. • 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. HP has corrected this potential vulnerability. • Fixes a problem where some crontab jobs would run multiple times in the same minute. • Fixes two cron problems: – The cron daemon does intensive logging and fills up the disk. – Multiple cron daemons continue to run and consume system resources due to the fact that after a user is deleted from the system there are still jobs running on the user's behalf. • Fixes a problem in viewing a variable subrange parameter from a Pascal module while using dbx. • Fixes three problems in dbx: – dbx stack trace is incomplete. – Assignment to a variable would fail after viewing a non-local symbol. – The use of vfork would raise a signal 66. • Fixes problems with the dbx kernel debug option when used on kernel core files from AlphaServer GS Series systems and other large memory systems.

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

Patch 1493.00 continued	• Provides bug fixes to the sys_check utility and updates the sys_check to version 114. • Provides the following changes to the sys_check utility: – Fixes the ra200info tool from core dumping. – Adds the sysconf program. • Fixes the following two problems with the collect information tool used by the sys_check utility: – A security hole where a user can become root. – Collect cannot start at boot time due to incorrectly handling SIGHUP signal. • Upgrades sys_check utiility to version 119.1 and provides the following changes: – Two NFS problems. – Fixes the ra200info tool from core dumping. – Utilizes Compaq Analyze when available. – Utilizes the new storage cliscript tool in place of hsxterm. – Updates the ASU section. • Fixes several problems with the collect command, and adds sysloging when collect suspends, resumes, or receives a signal. • Fixes errors generated by syscheck when NFS is not configured. • Upgrades sys_check to V120. • A potential security vulnerability has been discovered where, under certain circumstances, users can clobber temporary files created by shell commands and utilities (for example, under /sbin, /usr/sbin, /usr/bin, and /etc). HP has corrected this potential vulnerability. • Fixes the Collect's collector (/usr/sbin/collect) to correctly report the network interface load percentage. • Provides the /usr/lbin/mkstemp program which allows the mechanism to create a secure temporary file. • When using tip or any other method over the serial com lines to a receiver that sends frequent xoff/xon, characters are randomly repeated. • On a DECstation 1290.00/300, the second com port (tty01) does not get configured. An error message "ksh: /dev/tty01: cannot create" is displayed when the tty01 port is accessed. • Fixes a serial line hang and enables the halt switch on Eiger. • Fixes a kernel problem where proper locking/reference count management was not being performed. This could result in a "lock-terminate: lock held" system panic. • Fixes invalid malloc message in mfs. • Fixes a problem with the newfs command. When the newfs -N command was run on a mounted file system, it returned an error message similar to the following: newfs: /dev/rrz0c: is marked in the disklabel as in use by: 4.2BSD • Fixes a problem where a system panic will occur when accessing an ISO9660 format CD-ROM.

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

Patch 1493.00 continued	• Fixes a problem with CDFS. Data corruption occurs when reading beyond the end of a partition. • Fixes a problem in which the system may memory fault if the TCR/ASE server no longer had access to the CD-ROM device. • Fixes a problem where the system can panic with the panic string “secsize_resid < d_reclen” when accessing a defective CD-ROM. • Fixes a problem with CDFS. Fatal errors occur when trying to load data from a CDFS CD-ROM over NFS. • Fixes a panic seen when accessing the kio subsystem (such as with consvar) with improper arguments. The panic was caused by a kernel double-free, and would most likely be seen as a corruption in either the 64- or 96-byte bucket (buckets 2 and 16). • Fixes a problem where process accounting data was not written to the accounting file when it was on an NFS-mounted file system. • Corrects a “simple_lock: time limit exceeded” panic in softclock_scan(). • Fixes a kernel memory fault from socket code. The kernel memory fault results from failing to get a lock on a list of threads that have requested resources on a socket. • Corrects a problem where a signal is delivered, but not responded to, by the target process. • Fixes a panic of “get_color_bucket: empty buckets” when the sysconfig attribute private-cache-percent is non-zero. • A potential security vulnerability has been discovered where, under certain circumstances, users may gain unauthorized access. HP has corrected this potential vulnerability. • Fixes a problem with the mount command where it sometimes kills other processes. • Fixes problems with loadable drivers indicated by a maximum device number, lack of device number 0, or failure to reconfigure or reload a driver. • Fixes a problem in which mount would incorrectly fall back to Version 2 after certain errors had been encountered using Version 3. • Fixes an nfs/ufs/vm deadlock. While serving a client, the system running ASE/DT as an NFS server can hang with deadlock. • Fixes a problem in which the system may panic with the error message “kernel memory fault”. • Fixes several KZPCC RAID controller problems which in turn provides full support of the product. • Fixes a problem where applications using the fcntl() system calls may appear to hang. • Fixes “simple_lock: time limit exceeded” panics. • Fixes two problems: fork can fail to obtain swap space and the resource limitation on core files does not work as documented.

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

Patch 1493.00 continued	• Fixes a problem where the system can panic with the following console message: bs_bf_htop: invalid handle\n N1 = 0 • Fixes a system pause seen when doing a lot of I/O to UFS file systems. • Fixes a problem that causes system panics when thread_swappable is called with the current_thread as the target thread, when the thread is about to be swapped out. • This work provides functionality to allow detecting unlinked referenced files. • Fixes a problem with the map entry indexing scheme that results in the following panic: pmap_release_page: page not found • Fixes a problem in which certain invalid kernel address ranges may get ignored. This can result in invalid kernel memory accesses to be left unnoticed. • Fixes a problem that causes the Tru64 UNIX Version 5.0 update install procedure to exit with core dumps and /sbin/loader failures on a system. • Fixes a problem in the module core() that can cause a panic with the message: vrele: bad ref count • Fixes two separate problems: – A panic in the kernel with the following error message: simple_lock: time limit exceeded – A panic occurs when booting kernel interactively and setting the memlimit. The panic error message is as follows: kernel memory fault • Fixes a problem with kdbx. A core file created by kdbx was left in the root directory when recovering from a system crash. • Removes a Granularity Hint Regions (also called GH chunks) restriction which may be encountered on AlphaServer DS20 and ES40 systems running the Tru64 UNIX V4.0F release. This restriction can reduce performance for certain database applications. • Fixes several problems associated with Controller Reset (hard-error recovery) for the KZPCC backplane RAID controller. • Fixes a system hang condition. All NFS-related services may deadlock. • Fixes the database application core dumps when using truss/trace tools by remembering that COW has been set up on a shared pte and processes it correctly when a subsequent write access is made to the page.

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

Patch 1493.00 continued	• Fixes a data corruption problem that can occur when mapping to private regions. • Fixes a problem where AS1200 systems with more than three pairs of memory displays the following warning message on the console during boot: pmap_get_align: Unaligned memory hole found... Please reset the system to clear any previous memlimit • Fixes a kernel memory fault caused when a network application walked an inpq array. • Fixes a problem in which signals can be lost in multithreaded applications. • Fixes a problem that only occurs if real-time preemption is enabled and SMP test suites are run. • Fixes a problem that could result in a incorrect scheduling of threads when they were dispatched from the idle state. • Fixes a problem with virtual memory. When running the Oracle database, Oracle cannot detach from a shared memory segment. • Fixes single-step support in a debugger, such as Ladebug, for instructions that trap or fault. • Fixes an incorrect calculation for memory-usage-by-type when kmem_debug is set. • Fixes a simple_lock: hierarchy violation in sigq_abort() when lockmode is set to 4. • Fixes a system panic on multi-process systems (approximately 12 CPUs) with large memory (128GB). The system can panic with: panic: lock time on vm_page_free_lock • Fixes a problem in which unmounting an NFS mounted directory can cause a user process to coredump. • Fixes a problem where partitioned Turbolasers return incorrect CPU data for CPUs that are not in the partition. • Corrects a problem that was causing degraded performance of the WAN Support for Tru64 UNIX layered products. • Under certain conditions, when using Asynchronous I/O, the NULL pointer can be dereferenced in aio_unwire(), causing a kernel memory fault panic. This fix eliminates this possibility. • Fixes a problem where ubc_msync() may not flush out all the pages in the requested range. • Fixes var adm messages from truncation on larger configurations by raising the default size (4096) of msgbuf_size to 8192. • Fixes a problem where systems with the DUV40FAS0002-19991116 patch kit installed would run low on kernel memory after process accounting had been running for a while. • Corrects a problem where a mount(8) command failure caused the operating system to crash. Instead, the failure will now only cause the AdvFS file system domain to shut down.

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

Patch 1493.00 continued	• Fixes a problem on systems using the AdvFS file system, where the system can panic with the following panic string: del_clean_mcell_list: no primary xtnt record • Fixes an AdvFS domain panic that occurs with the following message on the console: load_x_cache: bad status from bs_refpg of sbm • Fixes a problem with AdvFS that will cause the system to panic with “kernel memory fault” in audit_rec_build(). • Fixes a problem where the statfs system call was reporting incorrect block usage on AdvFS filesets. As a side effect of this problem, the sendmail utility may sleep needlessly (waiting for space to become available). • Provides the following fixes and enhancements to AdvFS: – AdvFS volumes were not setting the default I/O byte transfer size to the preferred size reported by the disk drives. – AdvFS chvol read and write transfer size range was increased. – The read-ahead algorithm was modified to improve performance under certain conditions. • Fixes the problem where the system panics if AdvFS detects an inconsistency in the free list of mcells that is kept on a per-volume basis in an AdvFS domain. The panic string seen with this panic is as follows: alloc_mcell: bad mcell free list • Fixes a problem where update takes too long to sync mmap files when using an AdvFS file system. • Fixes the following two problems in AdvFS: – When a “log half full” or “log full” problem occurs, an entire system will panic. – The error message “ftx_bfdmn_recovery:bad record size\n N1 = 1” is received when the wordCnt, as returned by lgr_read, is not enough to hold the ftxDoneLRT record that precedes each log record in a log page. • Corrects a problem where a “can’t clear a bit twice” panic occurs after an unanticipated system crash and an improperly handled AdvFS recovery operation. • Corrects a problem in AdvFS that causes single-CPU systems to hang and causes multiple-CPU systems to panic with a “simple lock time limit exceeded” error specifying lock class name BfAccessTblMutex. • Corrects a problem in AdvFS where unmounting a domain that is already in a panicked state could result in the following system panic message: log_flush_sync: pinpg error\n N1 = 5 • Fixes a problem in AdvFS. AdvFS may skip file system recovery after aborted domain activation.

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

Patch 1493.00 continued	• Corrects a kernel memory fault that occurs when entering the mount -o dual command. Abbreviated stack: 9 _XentMM() 10 bs_bfdmn_sweep() 11 bs_bfdmn_activate() 12 bs_bfdmn_tbl_activate() 13 bs_bfset_activate_int() 14 bs_bfset_activate() 15 advfs_mountfs()
	• Fixes a problem that may cause panics to occur when msfs_getpage() receives an error return from fs_write_add_stg() when attempting to write to an AdvFS domain that is out of disk space.
	• Fixes a problem in AdvFS. A fileset is busy when attempting to unmount giving an EBUSY error even though the fileset has no open files.
	• ASE/Disaster Tolerance systems hang when a kernel vnode reclaim flushes a vnode’s modified data to disk and ASE/DT is currently suspending I/O requests.
	• Fixes a problem with making a msfs_putpage() call. The length argument may get its upper bits truncated, which will result in an incorrect length calculation.
	• Fixes a problem in the AdvFS system. A panic occurs with the following error message: lock_read: hierarchy violation
	• Fixes a situation in which a slight memory leak can occur when recovering AdvFS domains with mount.
	• Fixes a problem where a single CPU system using AdvFS can hang in cleanup_closed_list().
	• Corrects AdvFS problems involving clone filesets. The statfs syscall (used by df) was incorrectly returning zero blocks USED for clones. The read-ahead code was incorrectly passing up opportunities to do read-ahead on clone filesets, resulting in a large performance penalty.
	• Corrects two problems in AdvFS property list handling: – Creation of property lists entries in AdvFS filesets with no available mcells will result in kernel memory fault (kmf). – The get_proplist_entry function (used to disassemble the property list buffer returned by the getproplist system call) returned incorrect name length on property list names longer than 127 characters.
	• Fixes a problem with soclose() that caused permanent looping on exit while aborting pending connections at a TCP/IP listener socket.
	• When configuring the AlphaServer ES40, the ISA devices IDE and USB are not configured if a combo card is installed.
	• The system panics with a kernel memory fault when installing on an AlphaServer DS20.

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

Patch 1493.00 continued	• Fixes the following Compaq AlphaServer problems: – On the ES40 and DS20, nonfatal 680 environment machine checks are being logged as fatal/noncorrectable errors. – On the DS20, a fix has been made to the handling of power supply, temperature, and fan events so that they are reported correctly. – Provides support for the Compaq AlphaServer DS20E. • Allows the com1_environment variables to be stored in NVRAM. On a DS10 platform, resetting console baud rate to anything other than the rate it was running, a system panic occurs at boot. • Fixes various problems with the driver support for the Powerstorm 4D10T (ELSA GLoria Synergy) graphics board. • Provides the driver support for the PCI To Ethernet/Graphics Combo Adapter (3X-DEPVD-AA) (also known as the ITI6021E Fast Ethernet NIC 3D Video Combination Adapter, InterServer Combo, or JIB). • Adds additional error detection to the FC driver. • Updates the emx Fibre Channel driver to revision 1.12, adds support for the KGPSA-CA adapter, and also fixes the following problems: – In an ASE environment, the driver was not appropriately restoring the link state after a LIP, which typically occurs when the Fibre Channel cable has been unplugged. – When connected to the new Pleiades II switches, the switch ports would consume target IDs on the adapter’s SCSCI bus. – A kernel memory fault in routine emx_handle_els_request. – A system hang at boot up caused by infinitely trying to probe the Fibre Channel link. • Fixes a problem where, on systems with a Powerstorm 4D10T (ELSA GLoria Synergy) graphics board, the graphics were not reset to console mode (the blue screen) when the halt button was pressed. • Fixes several KZPCC RAID controller problems which in turn provide full support of the product. • Updates the emx Fibre Channel driver to Revision 1.17, correcting the following problems: – If connected to a switch that is part of a cascaded set of switches and is not the primary switch in the fabric, the host will never complete link initialization. – Occasionally, the link fails to initialize on the KGPSA-CA at boot. – If the cable connection between the switch and KGPSA-CA was unplugged and then replugged, the KGPSA-CA would fail to properly initialize the link and all FC connections would be terminated until the next system reboot. – Corrects some boot messages indicating mailbox command failures. • Fixes a kernel memory fault caused by a streams SMP race condition.

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

Patch 1493.00 continued	• Fixes the following Universal Serial Bus (USB) problems: – The USB mouse no longer functions after resetting the Xserver. – System panics may occur in error handling after USB device fails a request. – The USB device may not deconfigure properly when unplugged from the bus. – Problems that will prevent some USB devices from being configured at boot time. – A key on a USB keyboard will continue to repeat after being unplugged. – USB keyboards may transmit the incorrect keycode for several keys. • Fixes a system hang in which there is a large number of pending ioctls on the streams queue. • Fixes a panic in AdvFS which can have the following error messages: panic (cpu 1): bs_cow_pg: pin clone err panic (cpu 1): bs_cow_pg: cannot get blkMap • Fixes a kernel memory fault caused by a mishandling of multicast addresses on the FDDI interface. • Fixes a problem most frequently encountered by the ppp daemon /usr/sbin/pppd when the ppp connection is terminated. When run in debug mode, an exiting pppd will log a message similar to the following when the error is encountered: >> May 25 12:29:17 dragon pppd[2525]: ioctl(SIOCDIFADDR): Invalid argument • Fixes a kernel memory fault and an SMP race condition with the AltaVista Firewall 98 server on a multi-CPU system. • Fixes a problem when a default IP address and a cluster virtual IP address are interchanged after a network restart. The default interface address is used by all outgoing traffic and the alias address is only usable for the incoming packets. • Fixes a problem in which the system may panic with the error message “tcp_output REXMT”. • Fixes a problem where RCP commands issued from a Sun Solaris system to Compaq Tru64 UNIX may sometimes fail incorrectly with the error message “Connection reset by peer”. • Fixes a TCP performance problem if the TCP window scale option is turned off when using the HIPPI interface. • Fixes a system panic: tcphdr too big • Consists of changes necessary for the AltaVista Firewall 98 to pass ICSA certification. • Fixes a problem with packetfilter applications that use IP packets greater than 8K. • This patch involves virtual mac addressing. • Fixes a problem that caused AdvFS to incorrectly calculate metadata file size for files greater than 4 GB resulting in corruption on read and stat syscalls.

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

Patch 1493.00 continued	• Fixes a bug such that when fuser -k is issued on a dismounted NFS mount point in which some process is running, a hang will occur. • Fixes a problem in which an invalid error status is returned from the remove_entry system call. • Fixes a problem in which the interaction between NFS file systems and Smoothsync causes procprod to read stale data. • Fixes a kernel memory fault when accessing the vm_map_index hash table. • Fixes a simple_lock time limit exceeded panic due to an SMP race condition in namecache. • Fixes a problem that causes corruption in the floating point registers whereby the flag fields nxm_fp_owned are overwritten with 0s. • Fixes a problem in AdvFS. The system panics with a kernel memory fault. • Fixes a problem in AdvFS. A system panic occured with the following error message: panic: del_dealloc_stg(): cant ref bmt page • Fixes a kernel memory fault in VMAC code if_addnewaddr(). • Fixes a system hang that could last up to a few minutes with large files when performing synchronous I/O requests. • Fixes a system panic with the panic string: psig: catch not set • Corrects a kernel memory fault caused by rw3vp_cache passing a bad address to _OtsZero(). • Corrects a problem in which the perrmask register on Tsunami systems can be overwritten. • Fixes a problem where the output of a ps command, the PAGEIN column reports 0 for all processes. • Fixes a problem in which an application can hang because of an undelivered signal. • Fixes a problem in AdvFS. A panic occurs with the following error message: lock_read: hierarchy violation • 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 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 in which the POSIX interval timer is not resilient to clock slowdown caused either by NTP or by a backwards change of the clock. • Fixes a system panic that was seen on large configurations under a heavy load situation. • 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).

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

Patch 1493.00 continued	• Fixes a problem in AdvFS where putpage_lk/pg_busy deadlock causes hangs in the system. • Fixes several panics on systems with holes in memory. The error messages are listed below: panic: put_free_ptepage: invalid pvh state panic: kernel memory fault trap: invalid memory read access from kernel mode panic: not wired simple_lock: hierarchy violation • Adds a fix to VMAC functionality when used with NetRAIN. • Fixes a problem where the following can occur during a system panic: – System calls interrupts – mpsleep() returns an EINTR error when the panicstr is non-NULL – An infinite looping at a very high priority • Fixes AdvFS inconsistent quota problems and errors similar to the following appearing on the console: vmunix: chk_bf_quota: group quota underflow • Fixes a problem with verify. When verify is run on a brand new domain, NFS warnings are displayed even though no NFS related activity is being done. • Corrects a problem with the incorrect ordering of network interfaces which was resulting in network partitions. • Fixes a “lock_terminate: lock held” panic when deleting a process group. • Fixes an “unaligned kernel space access from kernel mode“ panic when doing a malloc from kmembucket 26, 896 byte bucket. The faulting virtual address will be the lock signature for thread_deallocate(). • Fixes a kernel memory fault in u_anon_faultpage() when it accesses the backing object for the anonymous page. • Fixes a problem where a root user was not allowed to check file access on behalf of a user without completely becoming the user. The functionality is needed by the ASU (Advanced Server for UNIX) product. • Fixes a panic in in_pcbfree() associated with ASE service failover. • Fixes a file system panic which has the following error message: syscall: complex lock owned • Fixes an AdvFS problem which caused the system to crash with a kernel memory fault. • Includes UFS delayed metadata mount option that fixes metadata intensive application performance. • Fixes a kernel memory fault seen under certain conditions when setting a thread’s priority.

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

Patch 1493.00 continued	• Fixes a race condition in the UBC code where a lookup is done on a page being invalidated (freed). • Fixes a race condition involving signals and threads that only happens on multiprocessor systems. • Fixes a problem with a kernel memory fault in AdvFS. • Fixes a problem where the operating system only looks in slot 0 for the primary CPU. • Corrects a KZPCC lock problem that is seen when a kernel is run with lockmode set to four. This patch also resolves a timing issue which prohibited the KZPCC product from being seen during boot on EV67 platforms. • Fixes a kernel memory fault caused by either one of the following conditions: – On EV6 platforms, when the debugger is used to view the OT_DEVMAP object mapping memory in I/O space that is mapped to a user process. – When routine pmap_coproc_exit_notify() modifies the pmaps' coproc_tbi function to be 0, a null pointer, while it is being checked by routine pmap_remove_all(). • Fixes a problem in which operations on NFS files can hang indefinitely. • Updates the emx Fibre Channel driver to revision 1.21 which corrects a Data Error that is seen when running with the latest Emulex firmware. This error corrupts data when reading from the disk. • Fixes a problem in which an invalid PCI entry in sysconfigtab can cause the system to be unbootable. • Fixes a problem in which a PCI bridge-based boot device may fail to configure on large I/O systems. • Fixes a problem where genvmunix does not boot on a system with an Atalla AXL200 card installed. • Fixes several problems specific to AlphaServer 1200 and AlphaServer 4100 systems. – The user.log file has the following message: redundant power supply failure – The messages file has the following intermittent messages: ERROR: i2c_read_temp: environmental monitoring error ERROR: i2c_read_fail_reg: environmental monitoring error ERROR: i2c_read_func_reg: environmental monitoring error – Systems were shutting themselves down displaying the following message: System has reached a high temperature condition. Possible problem source: Clogged air filter or high ambient room temperature.

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

Patch 1493.00 continued	• Modification to pci resource management to allow support behind pci bridges for the AXL200 card. • Fixes a system hang problem due to a bug in the NFS write gathering code. The code does not fully synch all writes. • Fixes a problem where applications on V4.0F systems can hang, looping in readdirplus(). • Fixes a problem in which an NFS system using a TCP connection can crash. • Fixes various performance problems with an upgrade to the Gigabit Ethernet driver Version 1.0.12. • Fixes a problem with relocating an TCR/ASE NFS service when one or many clients have the service mounted 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. • Fixes reply values for NFS writes which were causing protocol violations. • Fixes a problem in AdvFS in which a system that had already domain paniced results in a system panic. • Provides support for the DEGPA-TA (1000BaseT) Gigabit Ethernet device. • Fixes 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. • Fixes an AdvFS kernel memory fault caused by a race condition between migrate and chfile -L in bfflush_start. • Provides the device driver support for 3DLabs Oxygen VX1 graphics adapter. • Fixes a panic in the UFS file system which has the following error message: blkfree: freeing free block • Provides support for the DE600/DE602 10/100 Ethernet adapters and fixes the following problems in the driver shipped as part of the NHD kit: – A machine check that may occur shortly after boot or when receiving large amounts of data. – 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. • Fixes a panic in in_pcbfree() when NFS is implemented over TCP. • Fixes a problem with AdvFS. An AdvFS domain becomes inaccessible when using the mount -d option.

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

Patch 1493.00 continued	• Corrects a kernel problem which causes ping(8) to hang when using the -d flag. • Fixes a problem with AdvFS in which a hang occurs due to a deadlock between bsbuf.state and bmt extent map lock. • Fixes a problem in AdvFS. The following error messages can occur: panic: simple_lock: uninitialized lock kernel memory fault: simple_lock: minimum spl violation • Corrects a problem when a network interface is configured using a CIDR bitmask and lies in a certain address range; it could be unreachable by users on the local system and remote systems that choose not to use the routing table, but simply transmit on an interface. • Corrects a problem where there is a potential for a system panic in routine sbflush() if there is an attempt to flush a socket buffer while it is locked by another thread. • Fixes a problem with AdvFS where all processes are waiting for buffers causing the system to hang. • Fixes a hang or simple_lock_state_violation/simple_lock_fault panic in biodone. • This patch fixes a panic in AdvFS that has the following error message: ftx_fail_2: dirty page not allowed • Fixes two panics that have the following error messages: simple_lock: time limit exceeded simple_lock: lock already owned by cpu • Fixes a problem in AdvFS where user data may be lost when a clone file is migrated. • Fixes a problem where NFS does not update mtime and atime for special files and named pipes. Additionally, it fixes a problem that can cause an NFS client application to hang, or causes a “lock already owned by thread” panic when lockmode=4. • Fixes a problem where incorrect NFS client locking caused a KFM panic. • Fixes a problem where NFS clients may hang in the uninterruptable state. • Fixes a restart detection problem with the proplistd daemon. Prior to this fix, when mounting a relocated ASE NFS service with property lists, clients did not detect that the proplistd RPC port number had changed. Clients continued to use the proplistd RPC port number of the old ASE cluster member. • Prevents a possible NFS over TCP hang. NFS TCP threads will be blocked in sosbwait() causing the system to appear to be hung. • Addresses two problems with the ee driver for DE60x Ethernet cards. These problems affect all Tru64 UNIX systems containing ee cards. – Fixes a race condition where the card could stop receiving packets from the network under rare circumstances. – Fixes the lan_config user options -x and -s.

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

Patch 1493.00 continued	• Fixes a problem when using multiple subnets on a network interface; APR request packets sent by the system will contain the IP alias address in the sender field when that alias is in the same subnet as the requested IP address. • Fixes a problem when applications make IOCTL calls using an IP alias address on a network interface. • Corrects a problem in which a single application's creating and removing of files repeatedly in the absence of other applications working on the same fileset can cause poor update daemon performance due to a flawed kernel hashing algorithm. • 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 the setgid bit of a directory was not being set when created, if its parent directory has the setgid bit set. • Fixes hangs in AdvFS fileset operations such as clone creation and deletion when I/O errors or device full conditions resulted in the operation being undone. • Fixes a problem in which the system may panic with the panic string "Unaligned kernel space access from kernel mode". • Fixes a kernel memory fault from ufs_mount(). • Corrects a simple lock timeout seen when dealing with NFS loopback mounted file systems with large amount of dirty pages. • Fixes an unaligned access panic which occurs in malloc() in V4.0F systems, while allocating memory from the 512 byte memory bucket. It can occur on any type of file system. • Provides support for activating temporary data logging on a mount point. • Fixes a timing window where flushing data to disk can be incomplete when a system is going down, if more than one thread calls reboot() without first going through shutdown, /sbin/reboot, or /sbin/halt. • Addresses multiple issues for the KZPCC family of RAID Array 2000 (RA2000) controllers. – Errors seen when concurrent opens are issued to separate logical partitions on the same logical device. – Change to the preferred chunk size from 16 KB to 64 KB which may increase data transfer rates. • Fixes a problem in which the wrong status was returned from EEROM read. • Prevents a system panic from occurring while using AdvFS. • Fixes a problem with the driver for Gigabit Ethernet adapters (DEGPA-FA and DEGPA-TA) which prevented its use in a NetRAIN (Redundant Array of Independent Network Adapters) set. • Fixes a system hang caused by netisr queue corruption due to a race condition that is primarily encountered by third party drivers and layered products that call schednetisr_nospl().

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

Patch 1493.00 continued	• 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. • Corrects an AdvFS panic which can occur during a rmfset operation, causing the following panic string: rbf_delete_int: can’t find bf attributes • Fixes an issue with lightweight wiring of pages and shared memory regions. • Corrects a problem where a directory entry may be attempted to be changed to “.” and the code checks for this and prevents it from happening. • Fixes a lock hierarchy violation in AdvFs. • Increases the efficiency of the tcp_timers. • Fixes inaccuracy problems when using setrlimit/getrlimit with a threaded application. • Fixes a problem in which rmvol would hang in a wait state. • Fixes a hang in the UFS file system. • Fixes two problems with the consvar command: – Fixes consvar command problem with setting a boot device to a tape device. – Fixes consvar -g command to actually show the console settings as intended. • Fixes a memory leak when named pipes (FIFOs) are used. • Fixes a potential problem flushing data to disk when using data logging with sparse files. • Fixes a problem where threads can hang in x_load_in-mem_xtnt_map(). • Fixes a problem where cascaded switches can hang the system at failover time. • 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. HP has corrected this potential vulnerability. • CDFS media burned in 2001 shows the wrong dates. • Fixes a “u_anon_free: page busy” panic. • Fixes a problem where threads can hang while renaming files on NFS mounted file systems. • Fixes a “simple_unlock: lock not owned by cpu” panic in the biodone routine.

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

Patch 1493.00 continued	• Provides several fixes including: – Signal parent process to enable user notification of mount failure. – Return functionality to accept disk-type from user. – Exit if overlap detected and not being run interactively. – Do not do check_usage for -N option or mfs. – Move common variable declarations to header file. – Adjust fssize and references to it to handle larger file systems. • Fixes a kernel memory fault which occurs while using the tablet instead of the mouse. • Fixes a panic in AdvFS which has the following error message: panic: Unaligned kernel space access from kernel mode • Fixes an AdvFS hang that is caused by a thread waiting for flushCv notification and is holding resources that other threads want. This type of hang has been experienced when shutting the system down. • Fixes a problem that sometimes caused the system to select the incorrect IP source address for out-going connections when using IP aliases and subnetting on a network interface. • Fixes a system panic with panic string: “lock_terminate: lock held”. This is being caused by the table call which, when accessing an open file table from another task, was not doing the proper locking. • Corrects two problems: – The table() system will not abort connections properly if a tcb hash table number is greater than 1. – There was a kmf in option_scan due to SMP race between cfgmgr(CFG_OP_CONFIGURE) and sysconfigdb(CFG_OP_RECONFIGURE). The fix was to add a lock around access to cfg_db. • Fixes a bug in NFS that could possibly cause a kernel memory fault. • A kernel memory fault can occur on an smp machine when one thread is extending a clone frags file and another thread does a stat system call on a file with a frag. • Fixes an error handling path at label pg_error where entries made in the physical map should have been removed. • A potential security vulnerability has been discovered in the kernel where, under certain circumstances, a race condition can occur that could allow a non-root user to modify any file and possibly gain root access • Corrects an AdvFS problem where an on-disk variable wraps when more than 64K metadata entries are required to map the disk blocks of a file or metadata file. The side effects of this problem were data inconsistencies and an incorrect available size for the domain. • Fixes the following system panics: "Kernel Memory Fault" in function sth_close_fifo() when closing a vnode that belongs to a FIFO "simple_lock: time limit exceeded" in "spec_reclaim"

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

Patch 1493.00 continued	• Fixes a problem with vm_faults against anon objects mapped by multiple map entries. • Corrects the problem of a simple lock timeout due to POSIX timers and also corrects some inaccuracies of the POSIX realtime timers. • Fixes a problem where a system with a dual-mounted AdvFS file system can panic with the panic string, “bs_unpinpg: unpin sync with writeRef >1”. • The patch updates the emx driver to V2.01 and fixes the following problems: – A problem of unexpected tape I/O aborts – A panic of “can’t grow probe list” – Several kernel memory faults within the driver – Redundant adapter failures no longer panic the system – A problem of panicking with low memory resources – Stalling I/O during reprobing when a cluster member goes down • Corrects an AdvFS command problem. In rare cases, migrate programs (rmvol, balance, migrate, defragment) would fail to migrate a file due to E_PAGE_NOT_MAPPED. • Fixes a system panic with “malloc_check_checksum: memory pool corruption”. • Corrects a problem where an fcntl() with the FIFO parameter would return an errno=22 (Invalid Argument). • Corrects a problem which could result in a system panic on close() if the BPF default packet filter is in use. • Fixes a kernel memory fault in msg_rpc_trap. • Fixes a time loss problem seen on DS systems only when using console callbacks. The patch resynchronizes the clock when a time loss is detected. • Fixes a rare panic in the driver for the DE600/DE602 10/100 Ethernet adapter. • Fixes a problem where network interfaces can appear unresponsive to network traffic. • Fixes a kernel memory fault that can occur after a user issues kill -STOP. • Corrects a problem with ICMP redirect processing which resulted in incorrect ICMP redirect messages. • Fixes a panic of “malloc_leak: free with wrong type” when using kmem-debug-protect. • Fixes a problem in kernel threads where multi-threaded applications were allowed to start running prior to virtual memory mapping swapin. This was prevented by adding a flag to mark when the map is swapped out and prevents thread swapins until the flag is cleared. • Fixes a problem of the fverify -n flag creating directories. • Fixes kernel panics which can occur in the context of threaded applications. The panic string is “trap: invalid memory write access from kernel mode” and the faulting virtual address is always 0x0000000000000048.

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

Patch 1493.00 continued	• Fixes a problem with AdvFS that when mounting the file system with option -o dual a panic is caused. • Corrects a problem in the virtual file system that could cause panic with the panic string “kernel memory fault”. • Fixes a bug that can cause a panic when a system is powering down. • Corrects a problem with excessive receive overrun error messages from the FTA driver. • Fixes a bug that causes corruption of binary.errlog. • A potential security vulnerability has been discovered in networking where, under certain circumstances, a remote system can take over packets destined for another host. • Corrects a kernel memory fault panic in clntktcp_connect(). • Prevents the error message “local HSM Error: msgsvc: socket close failed” from being generated when an application closes the socket with return state 0. • Fixes numerous problems of accessing de-allocated and freed vnodes. • Fixes a problem where heavy use of a file system can result in “vnode table full” or “cannot create pipe” error messages. • Fixes a problem with crontab in which, when root runs crontab -e user, the user’s crontab file is edited and saved, but is not re-read by the cron daemon. Instead, root’s crontab file is re-read. • Fixes a problem where, when the user attempts to restore to a system configured with backplane RAID, btextract fails. • Fixes a problem where a system crash occurs at the end of a rmvol. The following panic string will be seen: panic (cpu 0): lsn_io_list: current lsn > hiflushlsn • Prevents addvol from adding invalid disks into a domain. • Fixes a problem caused when the Tru64 UNIX TCP layer prematurely closes a slow, but good connection with TCP reset. • Fixes three problems with the ee driver for DE60x Ethernet cards. These problems affect all Tru64 UNIX systems containing DE60x network interfaces. – A fix for a race condition that can cause a panic when a transmit timeout occurs. – A fix to improve error checking when allocating buffers. – A fix for DMA resource allocation to prevent a panic when a machine runs low on DMA resources. • Fixes a problem where the return value of unlink() call was not checked when two threads were trying to move a file to two different destination. Due to this, though one of the threads could unlink() the source file, there were no relevant error message displayed. • Corrects a potential system hang when the directory link limit is reached while creating sub-directories. This patch also corrects the erroneous reporting of success, when attempting to write beyond the file size limit using synchronized I/O. • Corrects a possible panic when auditing execve with exec_argp/exec_envp enabled.

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

Patch 1493.00 continued	• Fixes performance shortcomings in NXM thread replacement. • Fixes a kernel crash dump generation problem which resulted in the wrong page(s) being compressed/written. Without this fix, postmortem debugging may be difficult or impossible. • This fix will trap an inconsistent directory entry to prevent an infinite loop that might eventually cause a system hang. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. HP has corrected this potential vulnerability. • Corrects the problem where a user may experience a core dump when using csh from the Japanese locale. • Fixes a problem in fwrite() where it was failing when the total number of bytes to be written is larger than 2 GB. • Corrects the problem where the DLI queue stalls when there is no traffic in the TCP/IP or HDLC stacks. • Corrects a problem where the SNMP interface counter ifInUcastPkts occasionally decrements or jumps to an arbitrary, large value. • Corrects a failure in the safe_open() routine which caused symbolic links given by a relative path from the current working directory sometimes to give ENOENT errors incorrectly. • A potential security vulnerability has been identified in the HP Tru64 UNIX operating system which may result in non-privileged users gaining unauthorized access to files or privileged access on the system. This potential vulnerability may be in the form of a local and remote security domain risk. • Fixes a segmentation fault problem with long LOCPATH and LANG values. • Fixes a problem while expanding positional parameters in the bourne shell. The expansion “$@” should generate zero fields when there are no positional parameters specified for the shell function. • Fixed system panic and/or data corruption caused by changing fifo parameter pipe-databuf-size while fifo operations are in flight. • Fixes a ksh problem related to cleaning the process when a terminal is abruptly stopped. • Fixes the following problems in sh: – Service denial problem when a quoted here doc script is executed. – Problem with handling ELF files. – The shell variable $- was not holding the -C option when it was set to be on. – Problem with printing broken characters when the type builtin utility of sh is invoked in Japanese locale. • Fixes a kernel panic with “get_xm_page_range_info:kernel memory fault”. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised when a buffer overflow occurs in the BIND utility. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege. HP has corrected this potential vulnerability.

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

Patch 1493.00 continued	• Fixes a problem in audit_tool which appends nonsense characters to the audit information to the output of an execve event in brief mode. • Prevents a panic in fifo_write with the panic message "NULL fifo_bufhdr append pointer". • Fixes sync related processing of vnodes in AdvFS, NFS. • Provides protection against a class of potential security vulnerabilities called buffer overflows. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege. This patch allows a system administrator to enable memory management protections that limit potential buffer overflow vulnerabilities. • Fixes three problems with the alt driver for DEGPA Gigabit Ethernet adapters. These problems affect all Tru64 UNIX systems containing DEGPA network interfaces. • The improper scheduling of cron jobs related to the months that do not have 31 days is now corrected. • Fixes a problem that may cause the third command and other Atom-based instrumentation tools to fail. • Fixes an Asian language processing problem under the Korn shell. • Installs DECthreads V3.16-032 which fixes problems that may effect threaded programs using pthread_kill() on Tru64 UNIX V4.0F systems. • Fixes an sh problem while executing here document through command substitution. • Fixes a problem in the VM subsystem that could cause a crash with the panic string "vm_page_ssm_unwire". • Corrects an lpc regression in the lpc buffer overflow fix. • Fixes a bug that could cause a panic with the panic string "ubc_object_free: page still resident". • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised when a buffer overflow occurs in the ypmatch and traceroute utilities. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege. HP has corrected this potential vulnerability. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised when a buffer overflow occurs in the lpq, lpr and lprm commands. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands and the elevated privileges if the program file has the setuid privilege. HP has corrected this potential vulnerability. • Corrects a problem which had resulted in broadcast or multicast packets being processed multiple times on behalf of a NetRAIN device, once for each backup interface. • 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. HP has corrected this potential vulnerability.

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

Patch 1493.00 continued	• A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of file corruption due to the manner in which setuid/setgid programs core dump. HP has corrected this potential vulnerability. • Fixed the audit_tool search algorithm to differentiate between privileged and non-privileged uids, and to allow regular expressions in string searches. • NetRAIN virtual interface counters are not maintained properly, which affected reporting via netstat and snmp, and affects the proper operation of NetRAIN. • Fixes a problem with audit data not being displayed by audit tool, problems with file object selection/deselection and directories, and numa performance issues associated with auditing. • A potential security vulnerability has been identified in the HP Tru64 UNIX operating system which may result in a Denial of Service (DoS). This may be in the form of local and remote security domain risks. The following potential vulnerability has been corrected: SSRT2322 - BIND resolver (Severity - High) • Fixes a problem where opens would fail when running under heavy I/O load with the KZPCC. • Corrects a problem in which sh was using a high amount of CPU time. • 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. HP has corrected this potential vulnerability. • Fixes a problem for handling Floating Point Exception in collect. • 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. HP has corrected this potential vulnerability. • Fixes a Tru64 UNIX NFS server panic caused by receiving an illegal file access mode from an NFS client. • Fixes a potential problem where system responsiveness may be affected. • Corrects a problem where gated will no longer complain each time it attempts to send an OSPF HELLO packet and possibly fill up log files. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. A malicious user can attempt to subvert a program file that has the setuid or setgid privilege and possibly execute commands at an elevated privilege level. HP has corrected this potential vulnerability. • New lpd to fix /etc/hosts.lpd case sensitivity. For example, node.domain is treated the same as Node.Domain. • Fixes a problem where memory could retain execute permission on EV6 machines. Fixes a delete_pv_entry panic when kernel virtual address space has high usage.

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

Patch 1493.00 continued	• A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This may be in the form of network programs core dumping. HP has corrected this potential vulnerability. • Resolves kernel memory faults in the TCP/IP subsystem. • Enhances cron to do extensive logging. • Offlining a CPU with bound process(es) can lead to a “malloc_check_checksum: memory pool corruption” panic. • Fixes the following two ACL issues: – If multiple processes attempt to access the same file at the same time and access to the file should be allowed by an ACL on the file, access may be denied. – If the ACL on a file is corrupt, the corrupted ACL is passed into the kernel causing a variety of problems. • Corrects a problem found wherein the rmtmpfiles script would produce errors at startup of the form: dirclean: lstat failure for starting directory: /.osonly_tmp/: No such file or directory • Eliminates the compiler warnings in ksh. • Fixes a problem that caused the 4.3BSD socket interface to return incorrect values for IOCTL calls accessing IP alias address information. • Eliminates false directory lookup warning messages generated by an incorrect comparison caused by mismatched fileid variable types. The fix also slightly improves client caching performance. • A potential security vulnerability has been discovered where, under certain circumstances, users can clobber temporary files created by shell commands and utilities (for example, under /sbin, /usr/sbin, /usr/bin, and /etc). HP has corrected this potential vulnerability. • Fixes a regular expression performance problem in sed. • 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 access. HP has corrected this potential vulnerability. • Fixes an application core dump problem when the LANG environment variable is too long. • Fixes the predictable TCP Sequence Number. • Avoids a silent infinite loop in vdump by correcting the AdvFS system call OP_GET_BKUP_XTNT_MAP. The call will now return the valid xtntCnt when it fails due to E_NOT_ENOUGH_XTNTS. • Fixes a problem for locking on retry case for multi-threaded select/poll. A panic with the following stack trace is indicative of this problem: PANIC: thread_block: simple lock owned • A potential security vulnerability has been identified in the HP Tru64 UNIX operating system that may result in denial of service. This may be in the form of local and remote security domain risks. The following potential security vulnerability has been corrected: SSRT2266 IGMP (Severity - High)

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

Patch 1493.00 continued	• Fixes a problem in fread() where excessive I/O was taking place for large amounts of data, causing performance problems. It also addresses a failure in fread() to properly handle data sizes that have representations greater than 32 bits (2^32 of data). • 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 access. HP has corrected this potential vulnerability. • Fixes mbuf memory corruption that can cause kernel memory fault panics. • Prevents a possible lock hierarchy violation while opening a clone. • Fixes several problems with the collect utility. • Corrects a problem in AdvFS where it avoids a potential stranded log record in memory that does not get out to disk by fixing a race condition. • 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 access. HP has corrected this potential vulnerability. In addition the following changes were made: – shell inline input files are more secure – sh noclobber and new constructs added • Adds code to print greater than 61 UNIX domain sockets and change file read errors from /dev/kmem to ignore and continue in a running system. • Fixes a problem with fopen. The fopen command was returning “file not found” when there was insufficient memory available to allocate the FILE structure. The fopen command now returns “not enough space” for this case. • 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 access. HP has corrected this potential vulnerability. • Prevents a panic when I/O errors occur on an AdvFS directory page. • 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 access. HP has corrected this potential vulnerability. • Prevents segmentation faults when sia_ses_init is passed a malformed argument vector. • Fixes a potential security problem. • If an I/O fails and it may be helped by an AdvFS-initiated retry, a message will be written to the console providing information on how to retry. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised when a buffer overflow occurs in the sh utility. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege.HP has corrected this potential vulnerability.

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

Patch 1493.00 continued	• 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 access. HP has corrected this potential vulnerability. • Fixes a problem with the C shell (csh) so that it now correctly recognizes the backslash (\) meta character. • Fixes a problem with multi-threaded applications that can cause the application to consume 100% of the CPU usage time. • Corrects problems of audit_tool supplying incorrect, or insufficient data about an audit event. • Fixes a problem in the collect system monitoring tool when it is run in historical mode. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised when a buffer overflow occurs in the ksh utility. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege. HP has corrected this potential vulnerability. • Corrects a problem with csh(1) where if a non-root user performed an ls using wild card characters on a directory having permission 700, then it would display the invalid error message, “Glob aborted”. Now it displays the correct error message of “Permission denied”. • When ACLs are enabled and there is a Default Access ACL on a directory on an AdvFS file system, the permissions of symbolic links created in that directory will appear to be incorrect, even though access is not affected. • Corrects an NFS hang when the delayed option is used with the mount command. • Fixes two problems in the ee driver for DE60x 10/100 Ethernet adapters. These problems affect all Tru64 UNIX systems containing DE60x network interfaces • Fixes the new_wire_method (light weight wiring) issues for Oracle software. • Fixes the ARMTech kernel malloc invalid size panic. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised when a buffer overflow occurs in the telnetd daemon. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege. HP has corrected this potential vulnerability. • Corrects u_anon_free: page busy panics. • Provides protection against a class of potential security vulnerabilities called buffer overflows. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege. This patch allows a system administrator to enable memory management protections that limit potential buffer overflow vulnerabilities. • Corrects the tar program to properly handle unusual directory specifications.

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

Patch 1493.00 continued	• Fixes a problem with malloc() over-allocating memory from the kernel when malloc tuning variable __sbrk_override has been set to 1. • Prevents a kernel memory fault panic that would occur when the audit daemon is set to periodically dump the kernel audit buffers to the audit log file (auditd -d freq). • Corrects a problem which could result either in the panic of a cluster member or in inconsistent data when the sbcompress_threshold configurable is set. • Improves msync performance on files that are mapped with the MAP_PRIVATE flag. • 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. HP has corrected this potential vulnerability. • Fixes several potential system crash problems in the lfa driver for DAPBA and DAPCA ATM adapters. • Resolves a problem of not being able to view files on some CDROM media that is created by third party software. • Fixes a problem where decreasing the smoothsync_age does not always have an effect. • Fixes a problem in the kernel network subsystem that caused a kernel memory fault panic in the routine m_adj(). • Fixes a problem where in rare cases, the system would panic instead of failing gracefully. The panic message is: ftx_done_urdr: handle level N1 doesn't match ftx lvl N2 • Fixes a problem where in some cases, the system would report that there is no space left and would be unable to create files, even though there is disk space left and the BMT has not reached its maximal number of extents. • Fixes kernel memory faults caused by ufs_sync_int accessing an inactivated or de-allocated vnode. A Fixed Kernel Memory Fault panic could occur in irefresh while walking the mounted vnode list. • Provides a fix where the collect utility does not reproduce the CPU-type correctly. • Eliminates compiler warnings in ksh. • Installs DECthreads V3.16-030 which fixes problems that may affect threaded programs which use the fork() system call running on Tru64 UNIX V4.0F. • 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 access. HP has corrected this potential vulnerability. • Fixes a memory leak when dlclose'ing libraries in a threaded application. • Corrects a problem where df was showing negative values for large NFS file systems. • Fixes a kernel memory fault due to a bug in the kernel code.

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

Patch 1493.00 continued	• Fixes the following problems in tar/pax/cpio: – The tar command now checks and report any write errors. – The tar/pax/cpio commands have the capability to unalter the ctime of input files upon creation of an archive. It displays a warning message in case pax/cpio if it is unable to preserve the time of the input files. – Corrects the behavior of the tar -o option. – Fixes the cpio -m option, if the destination and source files have the same mtime. – The pax -l option has been corrected to create hard links properly. – The cpio -o option has been corrected not to corrupt extended uid file ownership. – Fixes the long file names handling in the tar command. – Fixes the pax command to handle ACLs on directories properly. • A potential security vulnerability has been identified in the HP Tru64 UNIX operating system which may result in non-privileged users gaining unauthorized access to files or privileged access on the system. This potential vulnerability may be in the form of a local and remote security domain risk. The following potential security vulnerability has been corrected: SSRT0845U stdio file descriptors (Severity - High) • Fixes a problem resulting in a system panic for applications that directly call nxm_get_bindings. • Prevents a race in msfs_umount. • 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. HP has corrected this potential vulnerability. • The TCP window has been increased from 96 KB to 500 KB for performance improvements. • The netisr thread dynamically estimates the reply size and subsequently reserves the space in the socket buffer. • A new timeout check has been added to notice when the data has not been acknowledged in 30-50 seconds and copies those buffers. This will allow the UBC to free up those mbufs and not tie them up. • Corrects a problem in which ksh fails to substitute the tilde (~) character for a user’s home directory after an assignment using the # or % characters has been used. • Allows the collect monitoring tool to recognize and gather KZPCC disk statistics. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised when a buffer overflow occurs. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege. HP has corrected this potential vulnerability. • The dirclean utility no longer attempts to remove the AdvFS .tags directory or the quota.group and quota.user files.

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

Patch 1493.00 continued	• Fixes a panic with simple_lock_timeout due to too many pages to scan in ubc_page_alloc(). • Fixes a problem with strerror where buffers could not be allocated. • Makes start-up scripts in /sbin/init.d world readable. • Fixes a kernel memory fault panic in the IP multicast loopback code. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised when a buffer overflow occurs in the chfn, chsh, or passwd utilities. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege. HP has corrected this potential vulnerability. • Addresses a kernel memory fault panic in malloc_thread(). • Fixes locking problems in vclean(). • Fixes heap and stack limitations in the older operating system versions required for SAP. • 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 access. HP has corrected this potential vulnerability. • Systems configured with VX1 graphics card will not return to the console when the halt button is pressed. The console is then unusable. • 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. HP has corrected this potential vulnerability. • Corrects a race condition which could result in a failure to set the modification time of a file. This occurs only on a ufs file system. • Keeps USB from initializing on systems where USB is not supported. • Adds an initialization of a variable setp necessary for an earlier patch. • Prevents panics caused by bad arguments to system calls. • Alleviates a temporary hang/pause condition seen when forking or running down an application with several child processes, from a parent process having an extremely large number of unique or discontigous memory allocations. • Corrects a problem in which ksh did not clean up the processes associated with a terminal once the window was closed. • sh now prints the correct msg when enhanced core file naming is on. • Fixes a problem with ksh. When a ksh menu is started from within a user’s .profile file, ksh will not stop when the telnet session is stopped. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. This could result in a panic with the string: “lock_clear_recursive: recursion not enabled.” HP has corrected this potential vulnerability. • Corrects the problem where telnetd leaves an extra udp port open.

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

Patch 1493.00 continued	• Under certain conditions, invalidating a portion of a very large file can make the file system appear to be hung. Any program trying to access the file system, ls for example, will hang until the file is invalidated. This will only happen when rt_preempt_opt=1. • This patch addresses two problems with the alt driver for DEGPA Gigabit Ethernet adapters. These problems affect all Tru64 UNIX systems using alt with vMAC or NetRAIN. – A fix for vMAC support. Prior to this patch, vMAC has not worked with DEGPA. – A fix to prevent two DEGPA adapters from getting the same MAC address in a NetRAIN configuration. • 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 access. HP has corrected this potential vulnerability. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised when a buffer overflow occurs in the dxterm utility. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege. HP has corrected this potential vulnerability. • Fixes memory leaks caused by certain type of scripts which is called in infinite loop. This consumes more virtual address space in the long run. • Corrects a Kernel Memory Fault that could result from an inp pointer disappearing when the listen socket is in the process of closing at the same time a new connection is establishing. • Fixes a problem where calling send() with the AIO flags set can cause the system to panic with a kernel memory fault in the aio_send code. • Corrects the behavior of more, when given both a non-existing file and a non-empty file with a long filename/pathname. • ARP request for a permanent ARP entry is ignored, user cannot connect from a remote system. • Fixes two code paths where someone could accidentally lookup the unspecified address (0.0.0.0), find an ARP entry for it, and start the timer ticking away on it eventually causing a panic. • A potential security vulnerability has been discovered in the HP Tru64 UNIX operating system that may result in a Denial of Service (DoS). This potential vulnerability may be in the form of local and remote security domain risks. The following potential security vulnerability has been corrected: SSRT2384 rpc (Severity - High) • Fixes a problem for excessive FIDS_LOCK contention observed when large numbers of files are using system based file locking. • 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 access. HP has corrected this potential vulnerability. • Corrects a problem which could result in an alias IP address being incorrectly promoted to being the primary address when another alias is removed.

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

Patch 1493.00 continued	• Fixes a problem where sh will not receive a SIGSEGV signal when you run type with a file path greater than 69 characters. • Fixes a problem with booting over the network (dataless management) and booting from a tape device. • Correction in cron to correctly handle backslash (\\) commands so that crontab and /dev/console output do not include backslashes. • Updates the emx driver to V2.03 and fixes a problem which could cause an emx driver panic during adapter resets. • Fixes a one byte gap/hole in the maximum size in the tar command before an extended header record is used (8589934591 (octal 77777777777)). • Allows fuser to display the reference flag. This flag indicates the type of reference made. For example, open, closed, unlinked, or mmapped. • Fixes an ISO9660 file system size limitation of 2.1GB and provides full capacity access to DVD-ROM media. • 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 access. HP has corrected this potential vulnerability. • Fixes an occasional panic that can be seen when reading from a process using Granularity Hints via procfs. • Fixes a problem when there is a hole in the virtual disk array. • Fixes a problem which can result in a panic, hang, or corruption from vnode deallocation during an unmount. This also fixes a VFS_UNMOUNT panic upon unmount. • 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 access. HP has corrected this potential vulnerability. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised when a buffer overflow occurs in the csh utility. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege. HP has corrected this potential vulnerability. • Fixes a problem of incorrect default route modification in which there is a race condition between gated startup and installation of static routes. • Fixes two possible panics in AdvFS: – Caused by bs_real_invalidate_pages. – Caused by bs_purge_dirty. • A potential security vulnerability has been discovered that may result in a denial of service (DoS) on RPC-based HP Tru64 UNIX servers with Enhanced Security (C2) enabled. This potential security vulnerability may be in the form of local and remote security domain risks. SSRT2412 portmapper with Enhanced Security (C2) enabled (Severity - High) • Avoids a domain panic when a E_CANT_ACCESS_LOG error is detected.

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

Patch 1493.00 continued	• Fixes a problem with RLIMIT_DATA process limits when running fsck on a large file system. • A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised when a buffer overflow occurs in the xdr library, which is used by the rpc library. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege. HP has corrected this potential vulnerability. • Fixes a “kernel memory fault” panic in the Virtual Memory subsystem on SMP systems. • Eliminates a Simple Lock Time Limit Exceeded due to the IoQueueMutex being held in bs_real_invalidate_pages. • A potential security vulnerability has been discovered in the HP Tru64 UNIX operating system, where under certain circumstances, system integrity may be compromised through improper file access (overwriting of files). This potential vulnerability is in the form of a local security domain risk. The following potential security vulnerability has been corrected: SSRT2301 uudecode (Severity - Medium) • Corrects a problem to avoid log inconsistencies. • Corrects a problem introduced in a prior patch which can result in a system panic when outputting through the packet filter. • Fixes segmentation errors that can occur when running SAS. • When the file system is full, now crontab will not be removing its entries and vi also will not be truncating the existing file. • Fixes an “unaligned access” panic when attempting to free or malloc memory from the 512 byte kernel memory bucket (bucket 5). • Fixes a kernel build failure seen during an Update Installation from CD-ROM. The problem affects systems whose default time zone (/etc/zoneinfo/localtime) is not in North or South America. • This patch provides protection against a class of potential security vulnerabilities called buffer overflows. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commands at the elevated privileges if the program file has the setuid privilege. This patch allows a system administrator to enable memory management protections that limit potential buffer overflow vulnerabilities. • Fixes a problem where the gettimezone script fails to present menus properly. • Fixes a problem that would generate a crash when running in lockmode 4. • Corrects a problem with large file systems (greater than 16K cylinder groups) created by newfs/mkfs/extendfs which can cause system panics when accessing data beyond cylinder group 16K. • Fixes a problem in the Network startup script where it would fail to configure an interface with an IP address. • Fixes a problem with csh picking the wrong message catalog entry from the translated message catalog when LANG was set to Japanese locale. • Fixes a possible security hole reported by SSRT2323 in QAR 96333.

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

Patch 1493.00 continued	• Fixes a problem encountered with the Bourne shell when a file name with a trailing slash (/) is used as an argument to the command. • Fixes a problem with NIS clients failing to connect to non-Tru64 NIS servers that only support the V2 NIS protocol. • Fixes various problems in the ee driver for DE60x Ethernet adapters. • Fixes an I/O hang condition on fibre channel. • Fixes a memory fault condition in the emx driver that occurs when responding to an inquiry command from a remote port in the fabric.

3 Summary of TruCluster Software Patches

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

Table 3–1 provides a summary of patches.

Table 3–1: Summary of TruCluster Patches

Patch IDs	Abstract
Patch 4.00 TCR160-004	**Patch:** Fix for Kernel Memory Fault On DRD Client Nodes **State:** Existing This patch fixes a kernel memory fault on the DRD client nodes just as or after the DRD server node has initiated MC2 hub failover.
Patch 7.00 TCR160-010	**Patch:** Fix for Reliable Datagram API **State:** Supersedes patch TCR160-001 (1.00) This patch corrects the following: • Reliable Datagram (RDG) messaging support. • RDG: bug fix to the completion queue synchronization protocol.
Patch 8.00 TCR160-011	**Patch:** doconfig may hang when running in TruCluster environment **State:** Existing This patch fixes two problems that could cause doconfig to appear to hang when running in a TruCluster environment.
Patch 33.00 TCR160-037	**Patch:** Fix for drdadmin problems **State:** Existing This patch fixes various problems with drdadmin to be user friendly.
Patch 34.00 TCR160-038	**Patch:** Fixes a limitation in ase_reconfig_bus **State:** Existing This patch fixes a limitation in ase_reconfig_bus. Now up to 99 buses can be reconfigured with this command.
Patch 36.00 TCR160-040	**Patch:** Fix for asedirector hang **State:** Existing This patch fixes a problem that could cause an NFS or Disk Service that has a hyphen (-) in the service name to end up unassigned after a disk failure. A side effect of the problem was that the asedirector would hang after the disk failure was corrected.
Patch 61.00 TCR160-054B	**Patch:** Fixes problems with the clu_ivp script **State:** Supersedes patches TCR160-009B (22.00), TCR160-021B (23.00), TCR160-022B (24.00), TCR160-031B (25.00), TCR160-036B (50.00), TCR160-047B (51.00) This patch corrects the following: • This is a performance improvement in the startup of start scripts. It will reduce the necessary system calls to start the scripts. • Corrects a problem with member add in a large environment.

Table 3–1: Summary of TruCluster Patches (cont.)

Patch 61.00 continued	• Corrects a problem which causes asemgr to core dump when modifying a single drd service to add more than 200 devices. • Fixes a problem that caused aseagent or asehsm to core dump when starting NFS and Disk Services that contain several LSM volumes. • Fixes a problem with extraneous compiler warnings about strdup() function calls from ASE. • Fixes a problem that caused the asemgr utility to not run when called from a program that is owned by root and has the setuid bit turned on. • Fixes three problems with the clu_ivp script. The script now checks to be sure that the cluster members are listed in the /etc/hosts file, and it no longer copies /var/adm/messages to /tmp. Copying the messages file to /tmp could result in the file system becoming full, and clu_ivp exiting with an error. The clu_ivp script now also checks the /var/adm/messages file for shared busses if none are listed in the configuration file.
Patch 65.00 TCR160-063	**Patch:** Unable to remove LSM volumes from DRD service **State:** Supersedes patch TCR160-003 (3.00) This patch corrects the following: • Fixes a problem where DRD permissions could be lost if a service is modified more than once. • Fixes a problem that prevented the removal of LSM volumes from a DRD service. The problem occurs when there are multiple LSM diskgroups in the service, and all of the volumes from one diskgroup were removed.
Patch 70.00 TCR160-056	**Patch:** TruCluster Production server hangs during boot **State:** Supersedes patches TCR160-017 (11.00), TCR160-027 (19.00), TCR160-032 (26.00), TCR160-062 (68.00) This patch corrects the following: • Fixes a problem where both nodes in a cluster will panic at the same time with a simple_lock timeout panic. • Fixes a kernel memory fault in rm_lock_update_retry(). • Fixes a problem which can cause the following panic: panic (cpu 0): rm_update_single_lock_miss: time limit exceeded • Fixes a problem that could cause an error to be returned when the TruCluster software should wait until a global lock is freed. • Fixes a problem that could cause a TruCluster Production server member to hang during boot, and can cause a “simple lock time limit exceeded” panic.
Patch 72.00 TCR160-067	**Patch:** Error msg if system contained unsupported controllers **State:** Existing This patch fixes a problem that caused an error message to be printed if the system contained unsupported controllers. The error message will now only be printed when running the command in verbose mode.

Table 3–1: Summary of TruCluster Patches (cont.)

Patch 74.00 TCR160-061	**Patch:** Access mode for a directory not set to default **State:** Supersedes patches TCR160-045 (41.00), TCR160-048 (44.00), TCR160-049 (45.00) This patch corrects the following: • Fixes a problem that caused the setting of the force unmount option to be incorrectly displayed by the asemgr utility. • Fixes a problem that caused shell errors if an invalid mount option was specified via the asemgr menu. • Fixes a problem that caused the device name for a UNIX File System (UFS) to not be displayed when modifying the force unmount option via the asemgr utility. • Fixes a problem that caused the access mode for a directory to not get set to the default after modifying them via asemgr.
Patch 76.00 TCR160-055	**Patch:** Problem causes mountd to exit without error **State:** Existing This patch fixes a problem that could cause mountd to exit without error during boot.
Patch 80.00 TCR160-070	**Patch:** Fixes problem with ASE_SNMPD_IGNORE_DISKS **State:** Existing This patch fixes a problem with the ASE_SNMPD_IGNORE_DISKS feature. After specifying a disk to ignore, the ASE service stop and add commands result in conflicting data. While the daemon.log reports apparent success (“hrm_dsk.c will ignore /dev/rzb10”) the error log reports a failure that indicates that the device is NOT being ignored (CAM “unit reserved error”).
Patch 88.00 TCR160-077	**Patch:** Fixes a problem that causes asedirector to core dump **State:** Supersedes patches TCR160-018 (12.00), TCR160-002 (2.00), TCR160-009A (9.00), TCR160-016 (10.00), TCR160-007 (5.00), TCR160-021A (13.00), TCR160-024 (16.00), TCR160-025 (17.00), TCR160-022A (14.00), TCR160-033 (29.00), TCR160-035 (31.00), TCR160-042 (38.00), TCR160-043 (39.00), TCR160-051 (47.00), TCR160-031A (21.00), TCR160-053 (49.00), TCR160-036A (32.00), TCR160-047A (43.00), TCR160-028 (27.00), TCR160-052 (48.00), TCR160-065 (52.00), TCR160-066 (53.00), TCR160-058 (54.00), TCR160-060 (55.00), TCR160-054A (56.00), TCR160-057 (57.00), TCR160-059 (59.00), TCR160-071 (78.00), TCR160-078 (83.00), TCR160-079 (84.00), TCR160-075 (85.00), TCR160-076 (86.00) This patch corrects the following: • Corrects a problem with Networker displaying garbage characters following service names. It occurs when the service name is 8 characters or greater. • Fixes two problems in the asedirector: – An ASE command timeout problem encountered by large ASE services. – An incorrect decision made by the asedirector as a result of a failed inquire services command. • This is a performance improvement in the startup of start scripts. It will reduce the necessary system calls to start the scripts. • Fixes a problem where the Host Status Monitor (asehsm) incorrectly reports a network down (HSM_NI_STATUS DOWN) if the counters for the network interface get zeroed.

Table 3–1: Summary of TruCluster Patches (cont.)

Patch 88.00 continued	• Fixes an ASE problem where, under certain circumstances, the service scripts could cause the ASE agent to loop during a start or stop service. • Corrects a problem with member add in a large environment. • Corrects a problem with TruCluster Available Server or Production Server cluster in which services have been started with elevated priority and scheduling algorithm. Under significant load this could lead to intermittent network and cluster problems. • Fixes a problem which caused a service not to start when there was a short network failure. This was seen only with long running stop scripts and special network configurations. • Corrects a problem which causes asemgr to core dump when modifying a single drd service to add more than 200 devices. • Fixes a problem that caused aseagent or asehsm to core dump when starting NFS and Disk Services that contain several LSM volumes. • Fixes a problem where the asemgr will hang as it continuously creates and kills multiple directors. • Corrects a problem that causes the ASE director to core dump during initialization. • Corrects a problem where modifying a service with a large number of DRDs will fail and a “could not malloc” message is seen in the daemon.log file. • Fixes a problem where the MEMBER_STATE variable always is shown as BOOTING instead of RUNNING. After first installing TCR, there is no way to have scripts know the MEMBER_STATE. This problem is cleared on a reboot. • Corrects a problem in which a network cable failure that corrects within 7 seconds of the failure can leave the services in a bad state. • Fixes a problem that caused the asemgr to get a memory fault when adding multiple services in a row. • Fixes a problem with extraneous compiler warnings about strdup() function calls from ASE. • Fixes a problem that caused the asemgr utility to not run when called from a program that is owned by root and has the setuid bit turned on. • Fixes a problem that can cause the TruCluster MIB daemon (cnxmibd) to core dump in Available Server environments. • Fixes a problem which caused an error message to be logged for the cnxmibd even though no error had occurred. • Fixes two issues with clusters: – When a cluster is brought up with ASE off, other members report it as UP and RUNNING instead of UP and UNKNOWN. – When a restricted service is running on a member, and asemember stop or aseam stop is executed, the service status is still reported as the member name, instead of Unassigned. • Fixes a problem where timeout values of greater than 30 seconds in /etc/hsm.conf would cause the ASE agent to fail at start up. • Fixes a bug where the aseagent will occasionally core dump on a SCSI bus hang.

Table 3–1: Summary of TruCluster Patches (cont.)

Patch 88.00 continued	• This patch fixes the following problems with the clu_ivp script: The script now checks to be sure that the cluster members are listed in the /etc/hosts file, and it no longer copies /var/adm/messages to /tmp. Copying the messages file to /tmp could result in the file system becoming full, and clu_ivp exiting with an error. • The script now also checks the /var/adm/messages file for shared busses if none are listed in the configuration file. • Fixes a problem that could cause the asedirector to core dump. • Fixes a problem that caused the asemgr to report that a disk, or mount point, was in multiple services when modifying a service name. • Fixes a problem with the ASE application from reporting an incorrect status while booting, after installation or while re-initializing the database. • Fixes a TruCluster 1.6 problem that when a member of the cluster is being port scanned, the asedirector, aseagent, and aselogger would core dump. • Corrects a problem in which ASE may attempt to start a service twice on the same member. This may cause service interruption. • Fixes a problem that caused the asedirector to hang and consume 100% of the CPU time if asemgr processes were modifying services from more than one node in the cluster at the same time. • Fixes a problem that caused the Host Status Monitor (asehsm) to hang. • Fixes a problem that caused error messages to be logged by the Host Status Monitor. The message should have been informational, rather than an error.
Patch 90.00 TCR160-080	**Patch:** Node crashes when holding an mc-api lock **State:** Supersedes patches TCR160-029 (20.00), TCR160-050 (46.00), TCR160-064 (63.00) This patch corrects the following: • Fixes a hang problem in a cluster when two nodes communicate using the mc-api and a third node, not involved in the calculation, is rebooted. • Fixes a problem that can cause a panic in mcs_wait_cluster_event() when using the Memory Channel API. • Fixes a problem with the Memory Channel API where, when a node crashes holding an mc-api lock, under certain circumstances the lock will not be released after the node crashes. • Fixes a problem in the Memory Channel API that can cause a system to hang.
Patch 92.00 TCR160-082	**Patch:** Routing info for ASE service not properly updated **State:** New This patch fixes a problem that could cause the routing information for an ASE service to not get properly updated when ASEROUTING is enabled, and a service relocates.

Table 3–1: Summary of TruCluster Patches (cont.)

Patch 94.00 TCR160-072	**Patch:** LSM disk information not updated in ASE database **State:** Supersedes patches TCR160-030 (28.00), TCR160-039 (35.00) This patch corrects the following: • Fixes a problem that would cause an error from awk(1) when modifying an ASE service that contained a large number of LSM volumes. The error would prevent the service from being properly modified. • Fixes a problem where LSM disk information was not properly updated in the ASE database when volumes were removed from a disk service. • Fixes a problem with updating ASE services which involves deleting and adding AdvFS domains on LSM volumes.
Patch 97.00 TCR160-074	**Patch:** Processes may get referenced several times **State:** Supersedes patches TCR160-008 (6.00), TCR160-023 (15.00), TCR160-044 (40.00), TCR160-046 (42.00), TCR160-073A (95.00) This patch corrects the following: • Fixes a problem in which a cluster node can panic with the panic string “convert_lock: bad lock state”. • Corrects a problem in which a failure in the session layer can cause DLM messages to become inconsistent, resulting in random DLM panics on the receiving member. • Fixes a problem that can cause a TruCluster member to panic during shutdown. • Fixes a bug where sometimes a certain shared sequence number will not be freed after use. • Fixes a problem where certain processes could get referenced several times. • Fixes an Oracle process hang if a node fails after receiving a rsbinfo message. • Fixes a DLM problem where two processes could take out the same lock.
Patch 99.00 TCR160-073B	**Patch:** clu_ivp script enhancements **State:** Supersedes patches TCR160-054C (67.00) This patch fixes three problems with the clu_ivp script: • The script now checks to be sure that the cluster members are listed in the /etc/hosts file. • The script no longer copies /var/adm/messages to /tmp. Copying the messages file to /tmp could result in the file system becoming full, and clu_ivp exiting with an error. • The script now checks the /var/adm/messages file for shared busses if none are listed in the configuration file. • Fixes an Oracle process hang if a node fails after receiving a rsbinfo message.
Patch 101.00 TCR160-081	**Patch:** clu_ivp does not recognize Emulex adapter **State:** Supersedes patch TCR160-041 (37.00) This patch corrects the following: • Fixes a problem where the Emulex Fibre Channel adapter was not recognized by clu_ivp. • Fixes a problem that could cause the clu_ivp script to loop forever if the network interface was not configured.

Table 3–1: Summary of TruCluster Patches (cont.)

Patch 103.00 TCR160-083	**Patch:** Fix for boot failure on a cluster **State:** Supersedes patch TCR160-034 (30.00), TCR160-068 (82.00) This patch corrects the following: • Fixes a problem which caused a boot failure on a cluster with a large number of shared SCSI buses. • Fixes a problem in clustered systems. It reduces the occurrences of tmv2_notify_cbf error messages in the errlog. • Fixes a possible system hang during shutdown due to a process having an active light weight wiring.
Patch 105.00 TCR160-084	**Patch:** Corrects a problem in memory channel **State:** New This patch corrects a problem in the memory channel that can cause communication to stop and erroneous network partitions.