# Tru64 UNIX Version 4.0G and TruCluster Server Products Version 1.6

## Patch Summary and Release Notes for Patch Kit-0004

**July 2003**

This manual describes the release notes and contents of Patch Kit-0004. 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*document.

**Hewlett-Packard Company**
**Palo Alto, California**

# Contents

# About This Manual

This manual contains information specific to Patch Kit-0004 for the Tru64™ UNIX Version 4.0G operating system and TruCluster™ Server Products Version 1.6 software. It provides lists of the patches contained in the kit and describes 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 the person who installs or removes the patch kit and for anyone who manages patches after they are installed.

## Organization

This manual is organized as follows:

*Chapter 1* Contains the release notes for this patch kit.

*Chapter 2* Summarizes the Tru64 UNIX operating system patches included in the kit.

*Chapter 3* Summarizes the TruCluster software patches included in the kit.

## Related Documentation

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

- Tru64 UNIX and TruCluster *Patch Kit Installation Instructions*
- Tru64 UNIX *Installation*
- Tru64 UNIX *System Administration*
- TruCluster Software Products*Installation*
- TruCluster Software Products*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:

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

Please include the following information along with your comments:

- The full title of this document.
- The section numbers and page numbers of the information on which you are commenting.
- The version of Tru64 UNIX or TruCluster products 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 HP technical support office. Information provided with the software media explains how to send problem reports to HP.

# 1

# Release Notes

This chapter provides information that you must be aware of when working with Tru64 UNIX 4.0G and TruCluster Software Products 1.6 Patch Kit-0004.

## 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 cluste 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 patch kit. We recommend that this kit not be placed in the `/`, `/usr`, or `/var` file systems because doing so may unduly constrain the available storage space for the patching activity.

- Permanent Storage Space

  Up to ~103 MB of storage space in `/var/adm/patch/backup` is 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 ~106 MB of storage space in `/var/adm/patch` is required for original files if you choose to install and revert all patches. See the *Patch Kit Installation Instructions* for more information.

  Up to ~2160 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

- Temporary Storage Space

  A total of ~250 MB of storage space is required to untar this patch kit. We recommend that this kit not be placed in the `/`, `/usr`, or `/var` file systems

because doing so may unduly constrain the available storage space for the patching activity.

- Permanent Storage Space

  Up to ~734 MB of storage space in `/var/adm/patch/backup` is 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 ~753 MB of storage space in `/var/adm/patch` is required for original files if you choose to install and revert all patches. See the *Patch Kit Installation Instructions* for more information.

  Up to ~1688 KB of storage space is required in `/var/adm/patch/doc` for patch abstract and README documentation.

  A total of ~184 KB of storage space is needed in `/usr/sbin/dupatch` for the patch management utility.

## 1.3 Release Note for TruCluster Software Products

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.

## 1.4 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 your installation.

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

  ./usr/.smdb./AFAADVANCED400.scp_extension     OSFBASE445     UNKNOWN
  ./usr/.smdb./AFAADVANCED401.scp_extension     OSFBASE445     UNKNOWN
  ./usr/.smdb./AFAADVANCED402.scp_extension     OSFBASE445     UNKNOWN
  ./usr/.smdb./AFAADVANCED403.scp_extension     OSFBASE445     UNKNOWN
  ./usr/.smdb./AFAADVANCED404.scp_extension     OSFBASE445     UNKNOWN
  ./usr/.smdb./AFAADVANCED425.scp_extension     OSFBASE445     UNKNOWN
  ./usr/.smdb./AFAADVANCED435.scp_extension     OSFBASE445     UNKNOWN
  ./usr/.smdb./AFAADVMAN400.scp_extension       OSFBASE445     UNKNOWN
  ./usr/.smdb./AFAADVMAN401.scp_extension       OSFBASE445     UNKNOWN
  ./usr/.smdb./AFAADVMAN402.scp_extension       OSFBASE445     UNKNOWN
  ./usr/.smdb./AFAADVMAN403.scp_extension       OSFBASE445     UNKNOWN
  ./usr/.smdb./AFAADVMAN404.scp_extension       OSFBASE445     UNKNOWN
  ./usr/.smdb./AFAADVMAN425.scp_extension       OSFBASE445     UNKNOWN
  ./usr/.smdb./AFAADVMAN435.scp_extension       OSFBASE445     UNKNOWN

    * no missing files detected
      -------------------------
```

## 1.5 Release Note for Tru64 UNIX Patches 771.00 and 773.00

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_V4.0G / 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, enter the following command:

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

libots3.so:

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

## 1.6 Release Note for Tru64 UNIX Patch 48.00

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 0 by default (`V_ROUND_enhanced` read is not activated), and `lsm_V_ROUND_enhance_proximity` is set to 512 by default.

Append tuning changes to the `/etc/sysconfigtab` file.. See the Tuning notes following for a description of the new `lsm_V_ROUND_enhanced` and `lsm_V_ROUND_enhance_proximity` tunable parameters. These tunable parameters 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, then only 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 parameters are as follows:

`sm_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. The default is 0.

`lsm_V_ROUND_enhance_proximity` — This variable indicates the proximity in which the last read and new read must 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. The default is 512.

## 1.7 Release Note for Tru64 UNIX Patch 750.00

This patch provides the X server support for the new 3DLabs Oxygen VX1 PCI graphics card. To obtain full support for this graphics card, you must also select Patch 255.00, 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`

## 1.8 Release Note for Tru64 UNIX Patch 196.00

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 I/O buses.

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.

We recommend 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`**

## 1.9 Release Note for Tru64 UNIX Patch 683.00

This release note describes 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 `/` is present at the end of an argument, then it would only act upon that particular directory and not the contents in the directory. For example:

```
tar xvf foo.tar dir1/ or tar tvf foo.tar dir1/
```

## 1.10 Release Note for Tru64 UNIX Patch 1008.00

The following contains updates to the `fixfdmn`(8) reference page.

fixfdmn(8) fixfdmn(8)
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 that 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 noncorrupt 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)

## 1.11 Release Note for Tru64 UNIX Patch 1017.00

The new Russian keyboard comes with five extra keycaps. To enable any of those extra keycaps, the user will need to modify `/usr/lib/X11/xkb/symbols/digital_russian`. 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 oringinal 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 ]
    };
```

## 1.12 Release Notes for Tru64 UNIX Patch 1107.00

These release notes contain information about Tru64 UNIX Patch 1107.00.

### 1.12.1 New sysconfig Tunable

**Note**

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 the Tru64 UNIX 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. With some expertise, 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 nonlocal 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)
```

### 1.12.2 audit_tool Switches

The `audit_tool` switches `-a`, `-r`, and `-u` now allow the user to specify a UID or one of the following values:

**n**

Selects all records with a nonprivileged UID.

**p**

Selects all records with a privileged (root) UID.

**u**

Selects all records with an unassigned UID (useful with the `-a` switch).

In addition, the `audit_tool` switches `-/` and `-s` now support regular expressions.

### 1.12.3 Security

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.

### 1.12.4 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 symbolic link, the presence of the symbolic link satisfies the criteria file exists whether or not the symbolic link 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 symbolic link whose target does not exist, sh returns an error rather than create the file. The >>| construct will suppress these checks and create the file.

### 1.12.5 ksh noclobber Behavior Clarified

For > with noclobber set, ksh will return an error rather than overwrite an existing file. If the specified file name is actually a symbolic link, the presence of the symbolic link satisfies the criteria file exists whether or not the symbolic link 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 symbolic link to a nonexistent file, ksh returns an error. This is a behavior change. Because ksh does not have a >>| redirection override, create the symbolic link target before accessing it through >> if you depend on appending through a symbolic link.

### 1.12.6 csh noclobber Behavior Clarified

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

### 1.12.7 sys_check(8) Update

The following is an update of the sys_check(8) reference page.

syscheck (8)

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 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 EVM(5) 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 offpeak hours. At 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 /etc files 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 a sys_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.

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 Server.

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 manual 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

## 1.12.8 mountd Reference Page Update

The following are updates 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.

## 1.12.9 UFS Delayed Metadata mount Option

This new `mount` option allows for disabling synchronous metadata writes on a specified file system. The new mount option 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 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 has two results. One, multiple updates to one block become only a one block write as opposed to multiple writes of the same block with traditional synchronous metadata update. Two, 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.

Do not use the `delayed` option on the `/` or `/usr` file systems. Use the `delayed` option only on file systems that do not need to survive across a system crash.

#### Usage

To enable the `delayed` option, run:

```
mount -o delayed <device> <mount point>
```

or

```
mount -u -o delayed <mount point>
```

### 1.12.10 Changes to the rexecd Reference Page

The following are updates for 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 set up 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.

### 1.12.11 3DLabs Oxygen VXI Graphics Card

This patch provides the driver support for the 3DLabs Oxygen VX1 graphics card. To obtain full support for this graphics card, you must also select Patch 750.00, 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 previous steps. The doconfig utility 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.

### 1.12.12 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 previous steps. The`doconfig` running on the original, unpatched `genvmunix` will not recognize the new Ethernet driver.

## 1.13 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 every time you reconfigure.

# 2

# Summary of Base Operating System Patches

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

**Table 2–1: Summary of Base Operating System Patches**

| Patch IDs | Abstract |
|---|---|
| Patch 2.00<br>OSF445CDE-002 | **Patch:** Fix for file permission problem<br>**State:** Existing<br>This patch fixes a problem in which file permissions allow any user to write to the /.dt/Trash/.trashinfo file. |
| Patch 3.00<br>OSF445CDE-003 | **Patch:** CDE does not re-create list of application groups<br>**State:** Existing<br>This patch fixes a problem where the Common Desktop Environment (CDE) Application Manager did not re-create the list of application groups at login. After customizing the application groups, users would see the old groups instead of the new groups. |
| Patch 7.00<br>OSF445X11-001 | **Patch:** ccedilla and Ccedilla characters do not display<br>**State:** Existing<br>This patch fixes the Turkish F keyboard problem, where the characters Ccedilla and ccedilla cannot be entered from the keyboard directly. |
| Patch 10.00<br>OSF445X11-004 | **Patch:** Provides missing compose definitions<br>**State:** Existing<br>This patch provides missing compose definitions when in ISO8859-15-based locales for the scaron, Scaron, zcaron, and Zcaron characters. |
| Patch 28.00<br>OSF445-024A | **Patch:** Adds missing prototype for stime function<br>**State:** Existing<br>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 31.00<br>OSF445-028 | **Patch:** Fixes a tftpd problem<br>**State:** Existing<br>This patch fixes a tftpd problem when responding to a broadcast read request and it adds the -b option to control whether to respond to any broadcasts. |
| Patch 33.00<br>OSF445-003 | **Patch:** Panic when running Classical IP over lfa ATM driver<br>**State:** Existing<br>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 37.00<br>OSF445-033 | **Patch:** quotactl prototype is now POSIX compliant<br>**State:** Existing<br>This patch changes the quotactl prototype in /usr/include/ufs/quota.h to meet POSIX standards. |
| Patch 46.00<br>OSF445-041 | **Patch:** Fix for if.h file<br>**State:** Existing<br>This patch fixes a typo found in the /usr/sys/include/if.h file. |

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

| | |
|---|---|
| Patch 48.00<br>OSF445-043 | **Patch:** Performance problem for round-robin sequential reads<br>**State:** Existing<br>This patch fixes a performance problem for round-robin sequential reads on LSM mirrored volumes. |
| Patch 50.00<br>OSF445-045 | **Patch:** Prevents vold from dumping core<br>**State:** Existing<br>This patch prevents /sbin/vold from dumping core during an execution of a volprint or other query command. |
| Patch 59.00<br>OSF445-054 | **Patch:** Cursor is displayed incorrectly<br>**State:** Existing<br>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 61.00<br>OSF445-056 | **Patch:** Fixes a problem with the psiop driver<br>**State:** Existing<br>Fixes a problem with the psiop driver that causes it to fail when vdump is used. The following error is displayed:<br><br>vdump : unable to write to device |
| Patch 62.00<br>OSF445-057 | **Patch:** Provides latest driver for PowerStorm 4D10T card<br>**State:** Existing<br>This patch provides the latest driver for the PowerStorm 4D10T (ELSA Gloria Synergy, SN-PBXGK-BB) graphics card and the latest graphics driver for the PCI To Ethernet/Graphics Combo Adapter (3X-DEPVD-AA). |
| Patch 63.00<br>OSF445-059 | **Patch:** Fixes a hang in shutdown process of system<br>**State:** Existing<br>This patch fixes a hang in the system shutdown process ("shutdown now") when a device has flow control switched off. |
| Patch 64.00<br>OSF445-006 | **Patch:** Fixes a kernel memory fault when using ATM<br>**State:** Existing<br>This patch fixes a kernel memory fault when using ATM. |
| Patch 80.00<br>OSF445-071 | **Patch:** Fix for memx command<br>**State:** Existing<br>This patch fixes a problem with the memx command where it improperly handles memory sizes of 2 GB or greater. |
| Patch 85.00<br>OSF445X11-005B | **Patch:** Fix for X server interaction with X font server<br>**State:** Existing<br>This patch fixes various problems with the X font server and with the X server's interaction with X font servers. |
| Patch 87.00<br>OSF445-024B | **Patch:** C++ functions do not properly resolve stime function<br>**State:** Existing<br>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 90.00<br>OSF445-087 | **Patch:** Corrects problems in the LAT driver<br>**State:** New<br>This patch corrects problems in the LAT driver which caused improper processing of the ioctl TCSBRK, as well as the generation of spurious characters when the libc routine tcdrain() was used. |

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

| | |
|---|---|
| Patch 95.00<br>OSF445-112B | **Patch:** Addresses performance and scalability issues<br>**State:** New<br>This patch addresses performance and scalability issues for highly contended threaded applications running on EV6 SMP machines. |
| Patch 97.00<br>OSF445-118 | **Patch:** Assembler generates incorrect error messages<br>**State:** Supersedes patch OSF445-044 (49.00)<br>This patch corrects the following:<br>• 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.<br>• Corrects a problem whereby the assembler would generate incorrect error messages for source programs, which produces a mix of hand-coded and assembler-generated relocation operands. |
| Patch 99.00<br>OSF445-089 | **Patch:** Fix for mailx<br>**State:** New<br>This patch corrects the problem so mailx(1) will work correctly if the -r and -s options are used together. |
| Patch 132.00<br>OSF445CDE-006 | **Patch:** dtlogin core dumps servicing srequests from XDMCP<br>**State:** New<br>This patch fixes a problem where the Common Desktop Environment (CDE) login daemon, dtlogin, core dumps occasionally when servicing requests from XDMCP clients such as X terminals or PCs running X servers. |
| Patch 147.00<br>OSF445-058B | **Patch:** Fixes reply values for NFS writes<br>**State:** New<br>This patch fixes reply values for NFS writes which were causing protocol violations. |
| Patch 157.00<br>OSF445-105 | **Patch:** Bootlink fails on Alphastations 600, 600A, 500/400<br>**State:** New<br>This patch fixes a problem in which the bootlink can fail on Alphastations 600, 600A, 500/400. |
| Patch 167.00<br>OSF445-093B | **Patch:** Fix for Enhanced Security problem<br>**State:** Supersedes patches OSF445-022B (86.00), OSF445-032B (88.00), OSF445-084B (165.00)<br>This patch corrects the following:<br>• Corrects a problem of the rsh command displaying a warning message instead of the rsh command output when C2 security is configured.<br>• 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 the /etc/auth/system/default file.<br>• 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.<br>• Fixes a problem for Enhanced Security configurations, where the Maximum Login Interval (u_max_login_intvl) field was being ignored for account templates. |
| Patch 169.00<br>OSF445-061 | **Patch:** Fixes a problem with advscan<br>**State:** New<br>This patch fixes a problem where advscan -a -g does not display bootable partitions properly. |

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

| | |
|---|---|
| Patch 182.00<br>OSF445-086 | **Patch:** Incorrect encoding for SysV Open call audit parameter<br>**State:** New<br>This patch fixes a problem where encoding for the SysV Open call audit parameter was incorrect. This could cause a system panic. |
| Patch 188.00<br>OSF445-092 | **Patch:** Fixes several problems in the tapex utility<br>**State:** New<br>This patch fixes the following problems:<br>• Accuracy of performance tests has been improved.<br>• The tapex exit status has been corrected.<br>• The tapex utility was fixed to determine eom status in Command Timeout Test and exit with nonsero status to indicate failure. |
| Patch 196.00<br>OSF445-135 | **Patch:** Fix for floppy disk<br>**State:** Existing<br>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 I/O buses. 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 203.00<br>OSF445-134 | **Patch:** fixso command causes segmentation fault<br>**State:** Existing<br>This patch fixes a problem with the /usr/ucb/fixso command that can cause a segmentation fault. |
| Patch 242.00<br>OSF445-173B | **Patch:** Supports temporary data logging on mount point<br>**State:** Existing<br>This patch provides support for activating temporary data logging on a mount point. |
| Patch 246.00<br>OSF445-122 | **Patch:** Fix for quotacheck -v command<br>**State:** Existing<br>This patch 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. |
| Patch 261.00<br>OSF445DX-008 | **Patch:** Updates Netscape Communicator to Version 4.76<br>**State:** Existing<br>This patch updates Netscape Communicator to Version 4.76 to fix missing default MIME types in Netscape Communicator 4.75. |
| Patch 283.00<br>OSF445DX-009 | **Patch:** dop cannot find application names which contain a dot<br>**State:** Existing<br>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 289.00<br>OSF445-142 | **Patch:** ATM setup script fails<br>**State:**<br>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 291.00<br>OSF445-199 | **Patch:** Fix for Memory Channel driver panic<br>**State:** Existing<br>This patch 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:<br>panic (cpu 0): rm_failover_if_necessary, both rails bad<br>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. |
| Patch 297.00<br>OSF445-147 | **Patch:** Fix for newgrp command<br>**State:** Existing<br>This patch corrects the problem where newgrp(1) fails if the file /etc/group contains multiple lines for one group. |
| Patch 299.00<br>OSF445-176 | **Patch:** Fix for parallel-processing support library<br>**State:** Supersedes patch OSF445-042 (47.00)<br>This patch fixes the following problems in the Compaq C compiler:<br>• A “virtual memory exhausted” error when compiling the Open Source encryption library OpenSSL.<br>• An optimizer problem in loop unrolling that caused an incorrect result under certain conditions.<br>• Various compiler crashes under certain conditions.<br>• A problem in bounds checking that caused a compilation to fail with a virtual memory exceeded error.<br>• A problem in the parallel-processing support library (libots3) that caused incorrect run-time results for an OpenMP program. |
| Patch 305.00<br>OSF445-148 | **Patch:** Security (SSRT0672U)<br>**State:** Existing<br>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. We have corrected this potential vulnerability. |
| Patch 307.00<br>OSF445-167 | **Patch:** Fixes automount handling of nogrpid option<br>**State:** Supersedes patch OSF445-036 (40.00)<br>This patch corrects the following:<br>• 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 rather than an error message.<br>• Fixes the automount handling of the nogrpid option. |
| Patch 313.00<br>OSF445CDE-009 | **Patch:** Fix for dtpad utility<br>**State:** Existing<br>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 315.00<br>OSF445-201 | **Patch:** Fix for ksh hang<br>**State:** Existing<br>This patch fixes a problem where the Korn shell (ksh) could hang if you pasted a large number of commands to it when it was running in a terminal emulator window (such as an xterm). |
| Patch 323.00<br>OSF445-160 | **Patch:** Corrects a memory leak in the XTI socket code<br>**State:** Existing<br>Corrects a memory leak in the XTI socket code |
| Patch 325.00<br>OSF445-152 | **Patch:** Prevents TurboLaser system panic<br>**State:** Existing<br>This patch prevents a panic on TurboLaser systems with a DE600 in PCI slot 0. Misidentification of the DE600 in PCI slot 0 causes data structure corruption.<br>TurboLaser systems include the following:<br>AlphaServer 8200<br>AlphaServer 8400<br>AlphaServer GS60<br>AlphaServer GS60E<br>AlphaServer GS140<br>A DE600 is a single-port 10/100 Mbps Fast Ethernet NIC. |
| Patch 331.00<br>OSF445-193 | **Patch:** Security (SSRT1-15, SSRT0713U)<br>**State:** Existing<br>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 333.00<br>OSF445-150 | **Patch:** rdist utility causes segmentation fault<br>**State:** Existing<br>This patch corrects a problem in the rdist utility which was causing segmentation faults on files with more than one link. |
| Patch 335.00<br>OSF445-132 | **Patch:** Kernel memory occurs occurs while using tablet<br>**State:** Supersedes patch OSF445-050 (56.00)<br>This patch corrects the following:<br>• Fixes a "lock_terminate: lock held" panic when deleting a process group.<br>• Fixes a kernel memory fault which occurs while using tablet instead of mouse. |
| Patch 360.00<br>OSF445-561 | **Patch:** addvol adds invalid disks into a domain<br>**State:** New<br>This patch prevents addvol from adding invalid disks into a domain. |
| Patch 362.00<br>OSF445CDE-029 | **Patch:** Corrects improper file access<br>**State:** New<br>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. We have corrected this potential vulnerability. |

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

| | |
|---|---|
| Patch 365.00<br>OSF445-475 | **Patch:** Fixes a correctable error reporting problem<br>**State:** Supersedes patches OSF445-080 (82.00), OSF445-129 (197.00), OSF445-127 (199.00), OSF445-206 (207.00), OSF445-346 (363.00)<br>This patch corrects the following:<br>• Provides enhancements for the GS-series platforms. The header information in Hierarchical Switch machine checks was incorrect. The early revisions of PCA hardware do not allow Window 3 DAC for DMA.<br>• Fixes a problem on AlphaServer GS80, GS160, and GS320 systems where under a specific set of unlikely circumstances it is possible for revision 4 PCA hardware to falsely report PCI hung bus errors. This will cause an uncorrectable hardware machine check and operating system panic. This patch must be installed if the hardware configuration includes any revision 4 PCA (IOP to PCI bus) adpaters.<br>• Fixes a problem on the Alphaserver GS80, GS160, and GS320 platforms where the system will issue an environmental warning and shut itself down when it reaches a critical temperature, even though this temperature is safe for the power supply.<br>• Fixes a kernel memory fault in GS series systems which have mixed revision PCI adapters.<br>• GS320/160/80 1.224 GHz CPU system ECC Enhancements for DTAG error logging.<br>• Fixes a correctable error-reporting problem that turns off the reporting of correctable errors forever on any CPU, except CPU 0, once throttling of correctable errors has begun. |
| Patch 367.00<br>OSF445-609 | **Patch:** Fixes improper file or privilege management<br>**State:** New<br>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 369.00<br>OSF445-597A | **Patch:** Fixes a problem in XTI caused by blocked mutex lock<br>**State:** New<br>This patch fixes a problem in XTI caused by a blocked mutex lock. Any thread attempting to send an abortive disconnect would hang. |
| Patch 371.00<br>OSF445-597B | **Patch:** Fix for XTI hang<br>**State:** New<br>This patch fixes a problem in XTI caused by a blocked mutex lock. Any thread attempting to send an abortive disconnect would hang. |
| Patch 593.00<br>OSF445-519 | **Patch:** Security (SSRT1-40U, SSRT1-41U, SSRT1-42U)<br>**State:** New. Supersedes patch OSF445-350B (591.00)<br>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.<br>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 596.00<br>OSF445-483 | **Patch:** Security (SSRT1-40U, SSRT1-41U, SSRT1-42U)<br>**State:** New. Supersedes patch OSF445-350C (594.00)<br>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.<br>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 601.00<br>OSF445-307 | **Patch:** Security (SSRT2275)<br>**State:** New. Supersedes patches OSF445-467 (597.00), OSF445-512 (598.00), OSF445-618B (599.00)<br>This patch corrects the following:<br>• 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.<br>• 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.<br>• 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.<br>• Fixes a problem in uucp. uucp between two Tru64 UNIX systems hangs when a uucp failure occurs. |
| Patch 604.00<br>OSF445-618C | **Patch:** Security (SSRT2275)<br>**State:** New. Supersedes patch OSF445-503B (602.00)<br>This patch corrects the following:<br>• 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.<br>• 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 607.00<br>OSF445-365 | **Patch:** Clarifies the output of shfragbf (AdvFS utility)<br>**State:** Supersedes patches OSF445-212B (350.00), OSF445-219B (605.00)<br>This patch corrects the following:<br>• 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.<br>• Corrects an AdvFS problem where an on-disk variable wraps when more than 64-K 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.<br>• Clarifies the output of shfragbf, an AdvFS utility. |
| Patch 609.00<br>OSF445-564B | **Patch:** Fixes a problem with audit data<br>**State:** New<br>This patch fixes a problem with audit data not being displayed by the audit tool, problems with file object selection/deselection and directories, and NUMA performance issues associated with auditing. |
| Patch 611.00<br>OSF445-618D | **Patch:** Security (SSRT2275)<br>**State:** New<br>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 613.00<br>OSF445-626B | **Patch:** Scripts in /sbin/init.d are now world readable<br>**State:** New<br>This patch makes startup scripts in /sbin/init.d world readable. |
| Patch 615.00<br>OSF445-412B | **Patch:** Security (SSRT1-40U, SSRT1-41U, SSRT1-42U, SSRT1-45U)<br>**State:** New<br>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 617.00<br>OSF445-481B | **Patch:** Corrects buffer overflow problem<br>**State:** New<br>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. |

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

| | |
|---|---|
| Patch 619.00<br>OSF445-481C | **Patch:** Corrects buffer overflow problem<br>**State:** New<br>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 621.00<br>OSF445-618E | **Patch:** Corrects buffer overflow problem<br>**State:** New<br>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 623.00<br>OSF445-436B | **Patch:** Security (SSRT1-40U, SSRT1-41U, SSRT1-42U, SSRT1-45U)<br>**State:** New<br>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 625.00<br>OSF445-626C | **Patch:** Fix for /sbin/init.d scripts<br>**State:** New<br>This patch makes startup scripts in /sbin/init.d world readable. |
| Patch 627.00<br>OSF445-350D | **Patch:** Security (SSRT1-40U, SSRT1-41U, SSRT1-42U)<br>**State:** New<br>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 629.00<br>OSF445-618F | **Patch:** Corrects buffer overflow problems<br>**State:** New<br>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 631.00<br>OSF445-626D | **Patch:** Update for /sbin/init.d scripts<br>**State:** New<br>This patch makes startup scripts in /sbin/init.d world readable. |
| Patch 633.00<br>OSF445-626E | **Patch:** Update for /sbin/init.d scripts<br>**State:** New<br>This patch makes startup scripts in /sbin/init.d world readable. |

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

| | |
|---|---|
| Patch 637.00<br>OSF445CDE-036A | **Patch:** Fixes buffer overflow problem<br>**State:** New Supersedes patches OSF445CDE-035A (634.00), OSF445CDE-010A (635.00)<br>This patch corrects the following:<br>• 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.<br>• 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.<br>• 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 641.00<br>OSF445CDE-036B | **Patch:** Fixes buffer overflow problem<br>**State:** New. Supersedes patches OSF445CDE-035B (638.00), OSF445CDE-010B (639.00)<br>This patch corrects the following:<br>• 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.<br>• 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.<br>• 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 643.00<br>OSF445-298 | **Patch:** OSF445-298<br>**State:** New<br>This patch fixes a problem in <sys/timeb.h> where the ftime() prototype was not available in the default compilation name space. |

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

| | |
|---|---|
| Patch 666.00<br>OSF445CDE-015B | **Patch:** Fixes improper file access<br>**State:** Supersedes patches OSF445CDE-001B (83.00), OSF445CDE-004B (103.00), OSF445CDE-020B (659.00), OSF445CDE-017B (660.00), OSF445CDE-023B (661.00), OSF445CDE-012B (662.00), OSF445CDE-038B (663.00), OSF445CDE-030B (664.00)<br>This patch corrects the following:<br>• Fixes a problem in which dtfile ICDE COSE tool does not work when TMPDIR is defined as /ldata/disk_local/tmp. The dtfile tool returns the following error:<br>/ldata/disk_local/tmp/sdtdbcache_AAAaadmma: Cross-device link<br>/ldata/disk_local/tmp/sdtdbcache_BAAaadmma: Cross-device link<br>Floating exception (core dumped)<br>• 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 as follows:<br>Desktop Not Initialized: Could not create Action/Datatypes database.<br>• 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.<br>• Fixes the dtprintinfo memory fault problem with long LANG value.<br>• 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.<br>• 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.<br>• 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.<br>• 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.<br>• 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. |

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

| | |
|---|---|
| Patch 668.00<br>OSF445-617 | **Patch:** grep now allows blank lines in the pattern file<br>**State:** Supersedes patches OSF445-034 (38.00), OSF445-078 (76.00), OSF445-155 (244.00)<br>This patch corrects the following:<br>• When the fgrep command is used with the -s option all output is suppressed.<br>• The command fgrep -f searchlist gets the following error message:<br>wordlist too large<br>if the searchlist is too long. In the test case it was 101.00 entries.<br>• The command fgrep -f searchlist displays datafiles verbatim if the searchlist has blank lines.<br>• Fixes a problem in which the grep command with the -w switch does not work as documented.<br>• 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 670.00<br>OSF445-419 | **Patch:** Provides mktemp(1) reference page<br>**State:** New<br>This patch adds the mktemp(1) reference page for the mktemp command. |
| Patch 673.00<br>OSF445X11-025 | **Patch:** Fixes a problem with XP1000 667 MHz system<br>**State:** Supersedes patches OSF445X11-005A (11.00), OSF445X11-006 (12.00), OSF445X11-018 (247.00), OSF445X11-013 (249.00), OSF445X11-033 (671.00)<br>This patch corrects the following:<br>• Fixes various problems with the X font server and with the X server's interaction with X font servers.<br>• Fixes a problem where the X server could core dump or get unaligned access errors when clients used the Multi-Buffering extension. This patch fixes a problem where the X server does not display windows properly for the 128th and subsequent clients.<br>• 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).<br>• Fixes a problem where the X server can grow excessively when accessing certain fonts.<br>• 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 675.00<br>OSF445-422 | **Patch:** Updates the mktemp(3) reference page<br>**State:** New<br>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 677.00<br>OSF445-557 | **Patch:** Fixes improper file or privilege management<br>**State:** New<br>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 679.00<br>OSF445DX-017 | **Patch:** OSF445DX-017<br>**State:** New<br>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 683.00<br>OSF445-584 | **Patch:** Fix for tar command<br>**State:** Supersedes patches OSF445-094 (116.00), OSF445-180 (256.00), OSF445-128 (257.00), OSF445-130 (259.00), OSF445-638 (680.00), OSF445-542 (681.00)<br>This patch corrects the following:<br>• Fixes a problem with the tar command. Inconsistencies occur when restoring a file system that contains more than two hard links to a file.<br>• Corrects pax/tar/cpio to properly extract explicitly specified files. When an archive contained a file with extended attributes and a different file (occurring later in the archive) was specified to be extracted, improper buffer pointer management resulted in the following display (the example uses tar):<br>tar: /dev/nrmt0h : This doesn't look like a tar archive<br>tar: /dev/nrmt0h : Skipping to next file...<br>tar: Memory allocation failed for extended data while reading : Not enough space<br>The directory option was similarly affected. In this case the information for the specified file was not reported.<br>• Fixes a problem with the tar and pax programs. These programs incorrectly append files to an existing archive and cause the file to become inconsistent. .<br>• 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.<br>• tar now checks and report any write errors.<br>• tar/pax/cpio have capability to unalter the ctime of input files upon creation of archive. And it displays warning message in case pax/cpio if unable to preserve the time of input files.<br>• Corrects the behavior of the tar -o option.<br>• Fixes the cpio -m option, if the destination and source files have same mtime.<br>• Corrects the pax -l option has been to create hard links properly.<br>• Corrects the cpio -o option to not corrupt extended uid file ownership.<br>• Fixes the long file names handling in tar.<br>• Fixes pax to handle ACL on directories properly.<br>• Fixes a one-byte gap/hole in the maximum size in the tar command before an extended header record is used (8589934591 (octal 77777777777)).<br>• Corrects the tar program to properly handle unusual directory specifications. |

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

| | |
|---|---|
| Patch 685.00<br>OSF445-493 | **Patch:** Security (SSRT2208)<br>**State:** New<br>A potential security vulnerability has been identified in the HP Tru64 UNIX operating system which may allow nonprivileged 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 687.00<br>OSF445-583 | **Patch:** fwtmp command displays invalid PID values<br>**State:** New<br>Now fwtmp will not display the invalid (negative) PIDs when the number of decimal digits of the PID value exceeds 5. |
| Patch 693.00<br>OSF445-590 | **Patch:** Corrects improper file or privilege management<br>**State:** New. Supersedes patch OSF445-620 (691.00)<br>This patch corrects the following:<br>• Addresses compiler warnings caused by calling function with too few arguments.<br>• 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 697.00<br>OSF445-482 | **Patch:** Corrects improper file or privilege management<br>**State:** New<br>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 699.00<br>OSF445CDE-037 | **Patch:** Corrects improper file access<br>**State:** New<br>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 703.00<br>OSF445-265 | **Patch:** Fixes a problem in latsetup<br>**State:** New<br>This patch fixes a problem in latsetup when the directory "dev/lat is not found. |
| Patch 705.00<br>OSF445-431 | **Patch:** Incorrect error msgs displayed for power regulator<br>**State:** New<br>This patch fixes a problem in which the system displays incorrect error messages regarding the power regulator. This problem is specific to Alphaserver 8X00 systems. |
| Patch 707.00<br>OSF445-565 | **Patch:** Corrects improper file access<br>**State:** New<br>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 709.00<br>OSF445-502 | **Patch:** Terminal code may block when allocating a buffer<br>**State:** New<br>This fix prevents "simple lock owned" panics. |

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

| | |
|---|---|
| Patch 711.00<br>OSF445DX-021 | **Patch:** Corrects improper file access<br>**State:** New<br>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 713.00<br>OSF445-537 | **Patch:** Corrects improper file or privilege management<br>**State:** New<br>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 719.00<br>OSF445X11-037A | **Patch:** Corrects improper file or privilege management<br>**State:** Supersedes patches OSF445X11-010A (153.00), OSF445X11-029 (714.00), OSF445X11-022A (715.00), OSF445X11-038 (716.00), OSF445X11-026A (717.00)<br>This patch corrects the following:<br>• Fixes various memory leaks in the Motif library (libXm) that could occur when creating and destroying Motif List, Text, and TextField widgets.<br>• Fixes a problem with Motif tear-off menus which may cause a core dump when the shell widget is destroyed.<br>• 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.<br>• Fixes a problem where XmGetPixmapByDepth may fail if a directory in the search path contatins a large number of files.<br>• Fixes a problem with the Motif ToggleButton Widget where, in some cases, it may not draw itself correctly.<br>• 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 723.00<br>OSF445X11-037B | **Patch:** Corrects improper file or privilege management<br>**State:** Supersedes patches OSF445X11-010B (155.00), OSF445X11-022B (720.00), OSF445X11-026B (721.00)<br>This patch corrects the following:<br>• Fixes various memory leaks in the Motif library (libXm) that could occur when creating and destroying Motif List, Text, and TextField widgets.<br>• 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. Compaq has corrected this potential vulnerability.<br>• Fixes a problem with the Motif ToggleButton Widget where, in some cases, it may not draw itself correctly.<br>• 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. |

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

| | |
|---|---|
| Patch 725.00<br>OSF445-369 | **Patch:** Fixes panic caused by moving power supply<br>**State:** Supersedes patches OSF445-018 (23.00), OSF445-088 (161.00)<br>This patch corrects the following:<br>• Corrects a problem in which the perrmask register on Tsunami systems can be overwritten.<br>• 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.<br>• Corrects a problem where moving the power supply from one slot to another can cause a panic. |
| Patch 727.00<br>OSF445DX-026 | **Patch:** Fixes buffer overflow<br>**State:** New<br>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 729.00<br>OSF445-497 | **Patch:** Corrects improper file or privilege management<br>**State:** New<br>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 731.00<br>OSF445DX-015 | **Patch:** Corrects improper file access<br>**State:** New<br>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 733.00<br>OSF445-499 | **Patch:** Corrects improper file or privilege management<br>**State:** New<br>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 735.00<br>OSF445-435 | **Patch:** Fixes curses.h and esnmp.h header files problem<br>**State:** New<br>This patch fixes an interoperability problem between the curses.h and esnmp.h header files. |
| Patch 737.00<br>OSF445-498 | **Patch:** Corrects improper file or privilege management<br>**State:** New<br>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 740.00<br>OSF445-635 | **Patch:** Eliminates compiler warnings in ln<br>**State:** New. Supersedes patch OSF445-603 (738.00)<br>This patch corrects the following:<br>• Corrects the behavior of ln -sf to address the issue caused when a symbolic link points to a nonexisting file.<br>• Eliminates compiler warnings in ln. |
| Patch 742.00<br>OSF445-399 | **Patch:** Fix for fsck command<br>**State:** New<br>This patch fixes a problem with RLIMIT_DATA process limits when running fsck on a large file system. |
| Patch 744.00<br>OSF445X11-031 | **Patch:** Corrects improper file access<br>**State:** New<br>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 746.00<br>OSF445-421 | **Patch:** Provides the safe_open(3) reference page<br>**State:** New<br>This patch adds the safe_open(3) reference page for the safe_open() routine in libc. |
| Patch 750.00<br>OSF445X11-030 | **Patch:** Correction for XCopyPlane<br>**State:** Supersedes patches OSF445X11-011 (194.00), OSF445X11-017 (274.00), OSF445X11-020 (747.00), OSF445X11-021 (748.00)<br>This patch corrects the following:<br>• Provides the Xserver library for the new 3DLabs Oxygen VX1 PCI graphcis card.<br>• Corrects blocks of erroneous pixels left behind when dragging CDE application manager icons on the desktop.<br>• Fixes an Xserver crash when using GTK on systems using the Oxygen VX1 graphics card.<br>• Corrects window corruption on an Oxygen VX1 graphics card if backing store/save unders are enabled.<br>• Corrects XCopyPlane to only copy the requested bitplane rather than all bitplanes on the Oxygen VX1 graphics card. |

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

| | |
|---|---|
| Patch 752.00<br>OSF445-612 | **Patch:** Fix for vdump and vrestore commands<br>**State:** Supersedes patches OSF445-038 (42.00), OSF445-090 (149.00), OSF445-177 (205.00)<br>This patch fixes the following vrestore problems:<br>• A previous patch caused incomplete restores.<br>• 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.<br>• A warning message is displayed and vrestore aborts if it fails to malloc space for a property list.<br>• A message that had been inserted at the end of the message file had the wrong message category (this could cause messaging confusion).<br>• An uninitialized variable in the code that restores property lists could cause malloc failures, memory faults, "error setting extended attributes", and infinite loops using the -l option<br>• Corrupted property list information could cause an infinite loop.<br>This patch fixes the following problems with the vdump command:<br>• Fixes a problem where the vdump command will sometimes store symbolic link files as directories in the vdump archive.<br>• Failed to flag compressed extended attributes records that are split across a vdump BLOCK boundary.<br>• 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.<br>• Corrects "Rewinding" message to avoid a segfault with Internationalized messages.<br>• Fixes vdump to pick up correct messages in all locales.<br>• Avoids some unnecessary function calls and thus allows faster vdumps.<br>This patch fixes the following problems with the vrestore command:<br>• 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".<br>• 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".<br>• Selective restore of hardlinked files is incomplete when they exist in different directories (fails to create a directory for the second occurrence of a file with the same inode number).<br>• The -Q option is added to vrestore to allow the user to request ignoring the quota files (thus avoiding the time it takes to process them).<br>• Fixes vrestore to pick up correct messages in all locales.<br>• Enables the display of bit file attributes with the -l option. |

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

| | |
|---|---|
| Patch 754.00<br>OSF445-492 | **Patch:** Corrects improper file or privilege management<br>**State:** New<br>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 756.00<br>OSF445-518 | **Patch:** Corrects improper file or privilege management<br>**State:** New<br>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 760.00<br>OSF445-613 | **Patch:** Corrects bfs command compiler warnings<br>**State:** New<br>This patch removes compiler warnings addressing outside of array bounds. |
| Patch 763.00<br>OSF445-296 | **Patch:** Corrects a problem with the os_mibs daemon<br>**State:** New. Supersedes patch OSF445-593 (761.00)<br>This patch corrects the following:<br>• Corrects 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.<br>• Corrects the problem where snmp getnext returns back the value of the wrongOID on queries in the FDDI MIB of os_mibs. |
| Patch 767.00<br>OSF445-604 | **Patch:** Provides dumprmt.msg message catalog file<br>**State:** Supersedes patches OSF445-021 (26.00), OSF445-645 (764.00), OSF445-478 (765.00)<br>This patch corrects the following:<br>• This patch fixes a problem in which the restore command can fail with the following error:<br>Cannot malloc space for property list<br>• Fixes dump to recognize LSM volumes correctly and not report random information when an error has occurred.<br>• Eliminates the /sbin/restore program's ignoring of property lists.<br>• Introduces dumprmt.msg for remote dump/restore messages. This new message catalog file is used in both rdump and rrestore programs. |
| Patch 769.00<br>OSF445DX-020 | **Patch:** Corrects improper file access<br>**State:** New<br>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 771.00<br>OSF445-539A | **Patch:** Provides V2.1-120 for libots3.so<br>**State:** Supersedes patch OSF445-230A (352.00)<br>This patch corrects the following:<br>• A problem in the parallel-processing support library (libots3) that caused incorrect run-time results for an OpenMP program.<br>• 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 773.00<br>OSF445-539B | **Patch:** Provides V2.1-120 for libots3.a<br>**State:** Supersedes patch OSF445-230B (354.00)<br>This patch corrects the following:<br>• A problem in the parallel-processing support library (libots3) that caused incorrect run-time results for an OpenMP program.<br>• 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 776.00<br>OSF445CDE-022 | **Patch:** Corrects improper file access<br>**State:** Supersedes patches OSF445CDE-007 (184.00), OSF445CDE-021 (774.00)<br>This patch corrects the following:<br>• Fixes a problem in which the Window Manager (dtwm) intermittently hangs on a system that uses multiple displays.<br>• Fixes a problem in the dtwm 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.<br>• 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 779.00<br>OSF445-267 | **Patch:** Fixes a problem in NetRAIN<br>**State:** New. Supersedes patch OSF445-328 (777.00)<br>This patch corrects the following:<br>• Corrects a problem with NetRAIN which prevents it from failing over to a backup interface if the primary interface is disconnected at boot time.<br>• Fixes a problem in NetRAIN. NetRAIN interface creation now fails if any of the requested standby interfaces do not exist |
| Patch 781.00<br>OSF445-449 | **Patch:** OSF445-449<br>**State:** New<br>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 784.00<br>OSF445DX-012 | **Patch:** Security (SSRT0785U)<br>**State:** Supersedes patches OSF445DX-001 (4.00), OSF445DX-002 (5.00), OSF445DX-003 (6.00), OSF445DX-004 (159.00), OSF445DX-013 (782.00)<br>This patch corrects the following:<br>• Fixes a problem in which the dxaccounts application does not allow users to be added to groups with a Group ID lower than the default minimum specified in the General Options dialog.<br>• Fixes the following cli/dxaccounts problems:<br>– The error message displayed when the Account Manager fails to start due to the detection of an Account Manager lock file (/etc/.AM_is_running) is not clear.<br>– The command uermod -D does not display the Expire date when it is set.<br>– Enabling to change root's login/uid through cli/dxaccounts utilities.<br>• Fixes a problem in which dxaccounts does not allow the system manager to add NIS users when the system is running enhanced security.<br>• 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.<br>• 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.<br>• Corrects the problem that causes the application dxaccounts to core dump when /etc/shells is a directory instead of a file. |
| Patch 789.00<br>OSF445-388A | **Patch:** Support for NEW_OPEN_MAX_SYSTEM file descriptors<br>**State:** New. Supersedes patches OSF445-245 (785.00), OSF445-417A (786.00), OSF445-264 (787.00)<br>This patch corrects the following:<br>• Warns a user of a possible hang that can occur when a program is linked to both libaio and libaio_raw.<br>• Prevents thread blocking forever when both libaio and libaio_raw are linked into the same image.<br>• Closes an aio_read()/aio_cancel() race condition.<br>• This patch is a backout of a previous fix to libaio which produces a warning when an application that was linked to both libaio and libaioi_raw is executed.<br>• Adds support for NEW_OPEN_MAX_SYSTEM (64 K) file descriptors to libaio. |
| Patch 792.00<br>OSF445-388B | **Patch:** Support for NEW_OPEN_MAX_SYSTEM file descriptors<br>**State:** New. Supersedes patch OSF445-417B (790.00)<br>This patch corrects the following:<br>• Prevents thread blocking forever when both libaio and libaio_raw are linked into the same image.<br>• Closes an aio_read()/aio_cancel() race condition.<br>• Adds support for NEW_OPEN_MAX_SYSTEM (64K) file descriptors to libaio. |

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

| | |
|---|---|
| Patch 794.00<br>OSF445-605 | **Patch:** Corrects exit status of sed when disk is full<br>**State:** New<br>This patch corrects the exit status of sed when the disk is full. |
| Patch 796.00<br>OSF445-560 | **Patch:** Corrects improper file or privilege management<br>**State:** New<br>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 802.00<br>OSF445-359 | **Patch:** Fixes od command hanging problem<br>**State:** New<br>This patch fixes an od command hanging problem. |
| Patch 804.00<br>OSF445-347 | **Patch:** Addresses multiple issues for RA2000 controllers<br>**State:** Supersedes patch OSF445-159 (311.00)<br>This patch addresses multiple issues for the KZPCC family of RAID Array 2000 (RA2000) controllers:<br>• Errors seen when concurrent opens are issued to separate logical partitions on the same logical device.<br>• Change to the preferred chunk size from 16 KB to 64 KB, which may increase data transfer rates.<br>• Fixes a problem where opens would fail when running under a heavy I/O load with the KZPCC. |
| Patch 807.00<br>OSF445CDE-019 | **Patch:** Corrects improper file or privilege management<br>**State:** New. Supersedes patch OSF445CDE-014 (805.00)<br>This patch corrects the following:<br>• 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.<br>• 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 809.00<br>OSF445-631 | **Patch:** Elminates compiler warnings in mkdir command<br>**State:** New<br>This patch eliminates compiler warnings in mkdir. |
| Patch 811.00<br>OSF445-588 | **Patch:** Corrects improper file or privilege management<br>**State:** New<br>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 813.00<br>OSF445-507 | **Patch:** Fixes truncating problem with sysconfig utility<br>**State:** New<br>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 817.00<br>OSF445CDE-043 | **Patch:** Corrects improper privilege management<br>**State:** New. Supersedes patches OSF445CDE-042 (814.00), OSF445CDE-040 (815.00)<br>This patch corrects the following:<br>• 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.<br>• 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.<br>• Fixes the message catalog for the CDE application dtprintinfo. |
| Patch 821.00<br>OSF445-627 | **Patch:** Corrects improper file or privilege management<br>**State:** New. Supersedes patches OSF445-450 (818.00), OSF445-259 (819.00)<br>This patch corrects the following:<br>• 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.<br>• 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.<br>• Allows whitespace in header field with the ps option -o. Multiple headers with whitespace can be given with the ps option -o. |
| Patch 824.00<br>OSF445-538 | **Patch:** Corrects improper file or privilege management<br>**State:** New. Supersedes patch OSF445-249 (822.00)<br>This patch corrects the following:<br>• Corrects the behavior of the sort(1) command which now checks for duplicates with the -c, -u, and -k options.<br>• 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.<br>• Addresses the problem where performing a sort on a large database using numerous keys fails during the consolidation phase of the temporary files. |
| Patch 826.00<br>OSF445-371 | **Patch:** Fixes a hang problem in the script command<br>**State:** New<br>This patch corrects a problem in which script would hang upon exit in a dfs configuration. |
| Patch 828.00<br>OSF445-396A | **Patch:** Security (SSRT0779U)<br>**State:** New<br>A potential security vulnerability has been discovered where, under certain circumstances, SNMP services can stop functioning. |

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

| | |
|---|---|
| Patch 830.00<br>OSF445-396B | **Patch:** Security (SSRT0779U)<br>**State:** New<br>A potential security vulnerability has been discovered where, under certain circumstances, SNMP services can stop functioning. |
| Patch 832.00<br>OSF445-521 | **Patch:** Corrects improper file or privilege management<br>**State:** Supersedes patch OSF445-117 (124.00)<br>This patch corrects the following:<br>• Fixes a problem that caused a kernel build failure when installing or deleting dupatch. This problem occurred on Compaq AlphaServer DS20 and ES40 systems.<br>• 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 834.00<br>OSF445-556 | **Patch:** Corrects improper file or privilege management<br>**State:** New<br>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 837.00<br>OSF445X11-034A | **Patch:** Fixes buffer overflow in X11 applications<br>**State:** Supersedes patches OSF445X11-015 (272.00), OSF445X11-002 (8.00), OSF445X11-008A (126.00), OSF445X11-032A (835.00)<br>This patch corrects the following:<br>• Fixes a memory leak in the libVX11 library for X applications where freeing a GC would not free all of its memory. This problem is most likely to occur in systems with a Cateyes graphics card (4D40T, 4D50T, 4D60T, or 4D51T).<br>• Fixes a problem in which some 8-bit characters cannot be entered directly from the keyboard when the Caps Lock setting is on.<br>• 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.<br>• 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 840.00<br>OSF445X11-034B | **Patch:** Fixes buffer overflow in X11 applications<br>**State:** Supersedes patches OSF445X11-008B (128.00), OSF445X11-032B (838.00)<br>This patch corrects the following:<br>• 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.<br>• 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. |

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

| | |
|---|---|
| Patch 842.00<br>OSF445X11-019A | **Patch:** Fix for security issue in X11<br>**State:** Supersedes patch OSF445X11-003A (9.00)<br>This patch corrects the following:<br>• Fixes a problem in which the svn widget of libDXm.so creates identical backgrounds and foregrounds.<br>• 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 844.00<br>OSF445X11-019B | **Patch:** Fix for security issue in X11<br>**State:** Supersedes patch OSF445X11-003B (84.00)<br>This patch corrects the following:<br>• Fixes a problem in which the svn widget of libDXm.so creates identical backgrounds and foregrounds.<br>• 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 846.00<br>OSF445-389 | **Patch:** Fixes premature termination of ofile kdbx extension<br>**State:** New<br>This patch fixes a premature termination of the ofile kdbx extension, and token length warnings when kdbx is invoked. |
| Patch 849.00<br>OSF445-455 | **Patch:** Fixes segmentation violation caused by ld command<br>**State:** Supersedes patches OSF445-161 (326.00), OSF445-156 (327.00), OSF445-169 (329.00), OSF445-243 (358.00), OSF445-228 (847.00)<br>This patch corrects the following:<br>• Fixes two problems in the linker where it would erroneously report "multiply defined symbol" errors or "unresolved symbol" errors:<br>– 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.<br>– Modifies the linker to cause it to rescan shared libraries before reporting unresolved symbols.<br>• Fixes two errors that occur when using the -f switch with the linker (ld):<br>– Using the -f switch produces link errors.<br>– Any unsupported switch beginning with -f gets interpreted to mean -f.<br>• Fixes a problem where the linker-defined symbol _fpdata would end up being undefined if it was referenced by a program but not used by the linker.<br>• Fixes a potential optimization problem with the linker (/bin/ld).<br>• Fixes two problems in the linker (ld):<br>– The .text symbol was being set incorrectly for -shared and -call_shared links.<br>– Five linker-defined symbols were not getting the correct type set in the Dynamic Symbol Table.<br>• 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. |

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

| | |
|---|---|
| Patch 851.00<br>OSF445-473 | **Patch:** Fixes kernel memory faults in DLI interrupt handler<br>**State:** New<br>This patch resolves kernel memory faults in the DLI interrupt handler. |
| Patch 853.00<br>OSF445X11-027 | **Patch:** Fixes a problem in the mwm window manager<br>**State:** New<br>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. |
| Patch 857.00<br>OSF445DX-018 | **Patch:** Fixes dxterm buffer overflow problems<br>**State:** New. Supersedes patches OSF445DX-019 (854.00), OSF445DX-024 (855.00)<br>This patch corrects the following:<br>• 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.<br>• 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.<br>• 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 859.00<br>OSF445-420 | **Patch:** Security (SSRT1-40U, SSRT1-41U, SSRT1-42U, SSRT1-45U)<br>**State:** New<br>This patch adds the dirclean(8) reference page for the /usr/sbin/dirclean utility. |
| Patch 861.00<br>OSF445-615 | **Patch:** Fixes problems found in accounting commands<br>**State:** New<br>This patch corrects the following:<br>• Resolved the differences in the CPU time and connect time, found during the conversion from ASCII format to binary and again back to ASCII of accounting reports.<br>• Resolved the differences in CPU time found in the output of acctcom and acctmerg commands for the same input file. |
| Patch 863.00<br>OSF445-629 | **Patch:** Update to which command<br>**State:** New<br>This patch fixes /usr/bin/which to take path information from the environment rather than ~/.cshrc if it is invoked from other than the C shell. |

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

| | |
|---|---|
| Patch 865.00<br>OSF445-632 | **Patch:** Corrects improper file or privilege management<br>**State:** New<br>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 869.00<br>OSF445-239 | **Patch:** Fix for xntpd buffer overflow problem<br>**State:** New<br>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 871.00<br>OSF445CDE-026 | **Patch:** OSF445CDE-026<br>**State:** New<br>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 873.00<br>OSF445-526 | **Patch:** Fixes a simple lock timeout violation<br>**State:** Supersedes patches OSF445-060 (65.00), OSF445-074 (77.00)<br>This patch fixes the following problems:<br>• Continuous resets when an I/O command is causing the resets<br>• Read capacity recovery failure<br>• Bad block replacement (BBR) processing<br>• A simple lock panic<br>• Fixes erroneous disk utilization values reported by the table system call. |
| Patch 875.00<br>OSF445-221 | **Patch:** Fixes a lock hierarchy violation<br>**State:** Supersedes patch OSF445-184 (337.00)<br>This patch corrects the following:<br>• Fixes DS10/DS20 performance problems introduced with the i2c driver by using thread blocking, rather than event_timeout() and DELAY().<br>• Fixes a lock hierarchy violation that could be seen with the generic kernel attribute lockmode turned on. |
| Patch 879.00<br>OSF445-562 | **Patch:** Corrects improper file or privilege management<br>**State:** New. Supersedes patches OSF445-452 (876.00), OSF445-568 (877.00)<br>This patch corrects the following:<br>• 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 882.00<br>OSF445-338 | **Patch:** inetd may block incoming connections<br>**State:** Supersedes patches OSF445-175 (293.00), OSF445-404 (880.00)<br>This patch corrects the following:<br>• Corrects a problem with inetd which could result in its termination without notice and without a core file.<br>• 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.<br>• Allows the socket listen backlog in inetd(8) to be set with the command-line option using the -l switch. |
| Patch 884.00<br>OSF445-594 | **Patch:** Corrects improper file or privilege management<br>**State:** New<br>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 886.00<br>OSF445-611 | **Patch:** Enhancement to the make command<br>**State:** New<br>/usr/opt/ultrix/usr/bin/make now checks dependencies on archive libraries properly. |
| Patch 888.00<br>OSF445-616 | **Patch:** OSF445-616<br>**State:** New<br>In a rolling upgrade, the merge used to fail for merging the .login file without informative messages on the cause. This has been corrected. |
| Patch 890.00<br>OSF445DX-025 | **Patch:** Corrects improper file access<br>**State:** New<br>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 895.00<br>OSF445-432 | **Patch:** Fixes a problem in binlogd daemon<br>**State:** Supersedes patches OSF445-194 (346.00), OSF445-326 (891.00), OSF445-397 (892.00), OSF445-533 (893.00)<br>This patch corrects the following:<br>• Fixes a problem in binlogd which overwrites adjacent header fields in an error record if the system's hostname is longer than 12 characters.<br>• Fixes a problem in which the binlog daemon can core dump if it attempts to recover events from a panic dump file containing invalid event data.<br>• Fixes a time formatting problem when Compaq Analyze is used to display events in time zones with a positive offset from GMT.<br>• Fixes a problem that may prevent a correct configuration table entry from being written to the binary error log on some systems. It also fixes a problem in which a misleading message may be displayed on older systems that do not support a configuration table. In addition to displaying this message, this bug causes binlog to malloc a randomly sized amount of memory that is never used, and if the malloc fails it displays an alarming malloc failure message.<br>• Causes the binary error log daemon, binlogd, to sync its logfiles before closing them on system shutdown. |
| Patch 897.00<br>OSF445-592 | **Patch:** Corrects improper file or privilege management<br>**State:** New<br>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 899.00<br>OSF445-587 | **Patch:** Corrects improper file or privilege management<br>**State:** New<br>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 901.00<br>OSF445DX-010 | **Patch:** OSF445DX-010<br>**State:** New<br>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. |
| Patch 903.00<br>OSF445-558 | **Patch:** : Corrects improper file or privilege management<br>**State:** New<br>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 906.00<br>OSF445-622 | **Patch:** Updates to the find command<br>**State:** Supersedes patches OSF445-014 (19.00), OSF445-470 (904.00)<br>This patch corrrects the following:<br>• Fixes a problem with the find command. Find fails to show filenames that start with a period.<br>• Corrects find -ls, which displayed an incorrect number of blocks.<br>• Corrects the find -ctime, -atime, -mtime behavior with respect to the + operations. Find + operations will match Greater Than, rather Greater Than or Equal To. |
| Patch 908.00<br>OSF445-515 | **Patch:** Corrects improper file access<br>**State:** New<br>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 910.00<br>OSF445-391 | **Patch:** Fix for salvage utility<br>**State:** Supersedes patch OSF445-051 (174.00)<br>This patch corrects the following problems:<br>• Fixes two infinite loops that could make salvage run forever.<br>• Removes garbage characters from symlink recovery in salvage.<br>• Fixes a problem that could cause salvage to core dump. |
| Patch 912.00<br>OSF445-366 | **Patch:** startslip unable to extract info from acucap file<br>**State:** New<br>This patch fixes a problem where startslip was not able to extract all the information from the acucap file. |
| Patch 915.00<br>OSF445X11-036 | **Patch:** Fix for ELSA Gloria Synergy graphics card<br>**State:** Supersedes patches OSF445X11-007 (13.00), OSF445X11-014 (270.00), OSF445X11-023 (913.00)<br>This patch corrects the following:<br>• 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), lines and images sometimes are not drawn correctly in scrolled windows.<br>• Fixes synchronization and drawing problems in the X server for the PowerStorm 4D10T (ELSA Gloria Synergy, SN-PBXGK-BB) graphics card.<br>• 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).<br>• The Elsa GLoria Comet card does not correctly draw nested shaded boxes or anything similar.<br>• Fixes a problem where, on systems with an ELSA GLoria Synergy graphics card, sometimes the X server would not draw stipple patterns correctly. |
| Patch 917.00<br>OSF445-559 | **Patch:** Corrects improper file or privilege management<br>**State:** New<br>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 919.00<br>OSF445-567 | **Patch:** Corrects improper file access<br>**State:** New<br>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 927.00<br>OSF445CDE-031 | **Patch:** Fixes buffer overflow occurring in mailcv<br>**State:** New<br>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 930.00<br>OSF445-271 | **Patch:** Fixes problems with de50x network interface cards<br>**State:** New. Supersedes patch OSF445-642 (928.00)<br>This patch corrects the following:<br>• Resolves a problem where some de50x network interface cards, under specific circumstances, may not send gratuitous arp packets .<br>• Fixes a problem with the 400ms delay upon network cable reinsertion, which could lead to temporarily held drivers. |
| Patch 937.00<br>OSF445-644 | **Patch:** Fix for collect command<br>**State:** Supersedes patches OSF445-114 (151.00), OSF445-563 (931.00), OSF445-348 (932.00), OSF445-447 (933.00), OSF445-380 (934.00), OSF445-234 (935.00)<br>This patch corrects the following:<br>• Fixes several problems with the collect command, and adds system logging when collect suspends, resumes, or receives a signal.<br>• Allows the collect monitoring tool to recognize and gather KZPCC disk statistics.<br>• Fixes several problems with the collect utility.<br>• Fixes a problem in the collect system monitoring tool when it is run in historical mode.<br>• Provides a fix where the collect utility does not reproduce the CPU type correctly.<br>• Fixes collect's collector (/usr/sbin/collect) to correctly report the network interface load percentage.<br>• Contains the fix for handling Floating Point Exception in collect. |
| Patch 939.00<br>OSF445-403 | **Patch:** Fix for Atom-based instrumentation tools<br>**State:** New<br>This patch fixes a problem that may cause the third command and other Atom-based instrumentation tools to fail. |
| Patch 941.00<br>OSF445X11-028 | **Patch:** Corrects improper file access<br>**State:** New<br>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 944.00<br>OSF445CDE-033 | **Patch:** Corrects buffer overflow in the dtterm utility<br>**State:** New. Supersedes patch OSF445CDE-034 (942.00)<br>This patch corrects the following:<br>• 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.<br>• 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 946.00<br>OSF445-548 | **Patch:** Corrects improper file or privilege management<br>**State:** New<br>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 948.00<br>OSF445-551 | **Patch:** Corrects improper file or privilege management<br>**State:** New<br>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 950.00<br>OSF445DX-022 | **Patch:** Corrects improper file access<br>**State:** New<br>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 954.00<br>OSF445-451 | **Patch:** Fix VM locking problem in procfs<br>**State:** Supersedes patches OSF445-048 (53.00), OSF445-185 (295.00), OSF445-522 (951.00), OSF445-217 (952.00)<br>This patch corrects the following:<br>• Fixes a kernel memory fault in procfs_get_s5_dir.<br>• Corrects a problem where attaching to a program with a debugger will cause periodic timers to be lost and will make the program hang.<br>• 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.<br>• Fixes a problem that made setuid programs unable to open themselves.<br>• FixesVM locking problem in procfs.<br>• Fixes a kernel memory fault related to ioctl PIOCMAP. |

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

| | |
|---|---|
| Patch 956.00<br>OSF445-549 | **Patch:** Corrects improper file or privilege management<br>**State:** New<br>This patch corrects the following:<br>• 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.<br>• Addresses the problem of coredump when the output of lint for a nonexisting file is supplied to error. |
| Patch 959.00<br>OSF445-610 | **Patch:** Corrects improper file or privilege management<br>**State:** New. Supersedes patch OSF445-465 (957.00)<br>This patch corrects the following:<br>• 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.<br>• Corrects the behavior of more, when given both a nonexisting file and a nonempty file with long filename/pathname. |
| Patch 961.00<br>OSF445-550 | **Patch:** Corrects improper file or privilege management<br>**State:** New<br>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 963.00<br>OSF445-628 | **Patch:** cut command now handles incomplete lines correctly<br>**State:** New<br>This patch fixes /usr/bin/cut to handle incomplete lines correctly. |
| Patch 965.00<br>OSF445-445 | **Patch:** Corrects improper file or privilege management<br>**State:** New<br>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 967.00<br>OSF445DX | **Patch:** Corrects improper file or privilege management<br>**State:** Existing<br>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 969.00<br>OSF445-540 | **Patch:** ddr_config utility now accepts larger values<br>**State:** New<br>This patch corrects the problem where /sbin/ddr_config does not accept values for ReadyTimeSeconds larger than 255. The new limit is 86400 seconds (24 hours). |

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

| | |
|---|---|
| Patch 972.00<br>OSF445CDE-013 | **Patch:** Security (SSRT0752U, SSRT0788U, SSRT0753U, SSRT0767U)<br>**State:** Supersedes patches OSF445CDE-008 (287.00), OSF445CDE-005 (180.00), OSF445CDE-001A (1.00), OSF445CDE-004A (101.00), OSF445CDE-020A (644.00), OSF445CDE-017A (645.00), OSF445CDE-023A (646.00), OSF445CDE-025 (647.00), OSF445CDE-039 (648.00), OSF445CDE-016 (649.00), OSF445CDE-027 (650.00), OSF445CDE-012A (651.00), OSF445CDE-011 (652.00), OSF445CDE-041 (653.00), OSF445CDE-038A (654.00), OSF445CDE-030A (655.00), OSF445CDE-024 (656.00), OSF445CDE-032 (970.00), OSF445CDE-015A (658.00)<br>This patch corrects the following:<br>• Fixes a problem on multi-head systems in which the unlock display only works if the default display is screen 0.<br>• 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.<br>• 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:<br>/ldata/disk_local/tmp/sdtdbcache_AAAaadmma: Cross-device link<br>/ldata/disk_local/tmp/sdtdbcache_BAAaadmma: Cross-device link<br>Floating exception (core dumped)<br>• 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:<br>Desktop Not Initialized: Could not createAction/Datatypes database.<br>• 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.<br>• Fixes the dtprintinfo memory fault problem with long LANG value. |

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

| | |
|---|---|
| Patch 972.00 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.<br>• Fixes a problem where a CDE session hangs at startup using localized .dt files located in ~/.dt/types directory.<br>• Fixes a potential security vulnerability in CDE Subprocess Control Service(dtspcd). dtspcd has a potential buffer overflow condition which may lead to unauthorized access. HP has corrected this potential vulnerability.<br>• 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.<br>• Fixes the problem of palette files not been read from /etc/dt/palettes.<br>• 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.<br>• 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.<br>• 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.<br>• 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.<br>• 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. |
| Patch 974.00<br>OSF445-569 | **Patch:** Fixes an IDE/ATA bus hang<br>**State:** Supersedes patch OSF445-091 (112.00)<br>This patch corrects the following:<br>• 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.<br>• Fixes an IDE/ATA bus hang caused by attempting to complete raw odd byte DMA transfers to/from IDE/ATAPI devices. |

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

| | |
|---|---|
| Patch 982.00<br>OSF445X11-024A | **Patch:** Fix for Xt that may cause mcc_iconic_map to crash<br>**State:** Supersedes patch OSF445X11-009A (118.00)<br>This patch corrects the following:<br>• 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.<br>• Fixes a problem in the X Toolkit library (Xt) that could cause the TeMIP Iconic_map Presentation Module application (mcc_iconic_map) to crash. |
| Patch 984.00<br>OSF445X11-024B | **Patch:** Fix for Xt toolkit library (Xt)<br>**State:** Supersedes patch OSF445X11-009B (120.00)<br>This patch corrects the following:<br>• 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.<br>• Fixes a problem in the X Toolkit library (Xt) that could cause the TeMIP Iconic_map Presentation Module application (mcc_iconic_map) to crash. |
| Patch 986.00<br>OSF445-474 | **Patch:** Corrects buffer overflow in the at command<br>**State:** New<br>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 988.00<br>OSF445-305 | **Patch:** Fixes an ATM signaling problem<br>**State:** Supersedes patch OSF445-146 (321.00)<br>This patch corrects the following:<br>• Fixes a problem of ATM signalling going into connection released after a system reboot.<br>• Fixes an ATM signaling problem. |
| Patch 990.00<br>OSF445-641 | **Patch:** Fix re_ioctl() case DIODCMD and DIODCDB<br>**State:** New<br>Fixes re_ioctl() case DIODCMD and DIODCDB. Changed to handle case where cmd transfer size has been changed to avoid kernel memory fault. |
| Patch 995.00<br>OSF445-405 | **Patch:** Fixes ATM simple_lock time limit exceeded panic<br>**State:** Supersedes patches OSF445-097 (133.00), OSF445-099 (135.00), OSF445-268 (991.00), OSF445-260 (992.00), OSF445-288 (993.00)<br>This patch corrects the following:<br>• When running ATM LAN Emulation, using more than four ATM NetRAIN interfaces can result in recursive calls, causing a "kernel stack not valid" halt.<br>• Fixes a problem of ATM LAN emulation failing to come up when using the ATM Meteor 351 board.<br>• Corrects a problem that could result in ATM/lane connection requests being dropped.<br>• Fixes a kernel memory fault when using ATM.<br>• Fixes a "simple_lock: time limit exceeded" panic when using ATM. |

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

| | |
|---|---|
| Patch 997.00<br>OSF445-520 | **Patch:** Corrects improper file or privilege mangement<br>**State:** New<br>A potential security vulnerability has been discovered, where, under certain curcumstances, system integrity may be compromised. This may be in the form of improper file or privilege mangement. HP has corrected this potential vulnerability. |
| Patch 1008.00<br>OSF445-387 | **Patch:** Fix for fixfdmn core dump problem<br>**State:** New. Supersedes patches OSF445-240 (998.00), OSF445-376 (999.00), OSF445-525 (1000.00), OSF445-256 (1001.00), OSF445-390 (1002.00), OSF445-640 (1003.00), OSF445-429 (1004.00), OSF445-382 (1005.00), OSF445-329 (1006.00)<br>This patch corrects the following:<br>• Provides support for the /sbin/advfs/fixfdmn utility. The /sbin/advfs/fixfdmn utility is a tool that is used to check and repair corrupted AdvFS domains. Refer to the Release Notes for a complete description.<br>• Allows fixfdmn to modify only one page of the transaction log.<br>• In some cases an inconsistent deferred delete list would cause fixfdmn to fail.<br>• Fixes a core dump if the log extents were on different pages in the RBMT. Handles new On Disk Structures introduced in V5.1B.<br>• Prevents fixfdmn from changing filesizes unnecessarily.<br>• Allows fixfdmn to fix a rare inconsistency case in the RBMT/BMT0.<br>• The fixfdmn utility will now remove full frag groups from the free frag list in the fileset frag file.<br>• fixfdmn could core dump on a rare inconsistency.<br>• fixfdmn 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 in the tag file.<br>• 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 OS. |
| Patch 1010.00<br>OSF445-255 | **Patch:** Fixes a kernel memory fault in pgrp_ref<br>**State:** New<br>This patch fixes a kernel memory fault in pgrp_ref. |
| Patch 1013.00<br>OSF445-553 | **Patch:** Fix for ftp open command<br>**State:** New. Supersedes patch OSF445-555 (1011.00)<br>This patch corrects the following:<br>• A potential security vulnerability has been discovered, where under certain circumstanes, system integrity may be compromised. HP has corrected this potential vulnerability.<br>• Corrects a bug in the ftp(1) open command. The optional port argument now accepts port numbers between 32768 and 65535. |
| Patch 1015.00<br>OSF445-491 | **Patch:** Corrects improper file or privilege management<br>**State:** New<br>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 1017.00<br>OSF445X11-035 | **Patch:** Updated keyboard map for Russian 3R-LKQ48-BT keyboard<br>**State:** New<br>This patch provides an updated keyboard map for the Russian 3R-LKQ48-BT keyboard model. |
| Patch 1019.00<br>OSF445-487 | **Patch:** Corrects improper file or privilege management<br>**State:** New<br>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 1021.00<br>OSF445-489 | **Patch:** Corrects incorrectly installed signal handler<br>**State:** Supersedes patches OSF445-022A (27.00), OSF445-032A (36.00), OSF445-084A (162.00), OSF445-093A (164.00)<br>This patch corrects the following:<br>• Corrects a problem of the rsh command displaying a warning message instead of the rsh command output when C2 security is configured.<br>• 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 the /etc/auth/system/default file.<br>• 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.<br>• Fixes a problem for Enhanced Security configurations, where the Maximum Login Interval (u_max_login_intvl) field was being ignored for account templates.<br>• Corrects the problem of an incorrectly installed signal handler when Enhanced Security is enabled. |
| Patch 1023.00<br>OSF445-270 | **Patch:** Provides fix for the BPF default packet filter<br>**State:** New<br>This patch corrects a problem that could result in a system panic on close() if the BPF default packet filter is in use. |
| Patch 1025.00<br>OSF445-414 | **Patch:** Provides the ckfsec(1) reference page<br>**State:** New<br>This patch delivers the ckfsec(1) reference page. |
| Patch 1027.00<br>OSF445-589 | **Patch:** Corrects improper file or privilege management<br>**State:** New<br>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 1029.00<br>OSF445-331 | **Patch:** Security (SSRT0664U, SSRT0762U)<br>**State:** Supersedes patches OSF445-121 (340.00), OSF445-153 (342.00)<br>This patch corrects the following:<br>• 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.<br>• Corrects a problem with the ftpd daemon which could result in PC ftp clients hanging when transferring some files in ASCII mode.<br>• Fixes a globbing problem with ftp where numerous concatenated asterisks in a directory search would cause ftp to fail and drop the user into a shell. |
| Patch 1033.00<br>OSF445-547 | **Patch:** Corrects improper file or privilege management<br>**State:** New<br>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 1035.00<br>OSF445-384 | **Patch:** Security (SSRT0794U)<br>**State:** New<br>A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be compromised. HP has corrected this potential vulnerability. |
| Patch 1037.00<br>OSF445-413 | **Patch:** Provides the ckfsec utility<br>**State:** New<br>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. |
| Patch 1039.00<br>OSF445-252 | **Patch:** Device inaccessible after aseagent daemon interup<br>**State:** Supersedes patch OSF445-055 (60.00)<br>This patch fixes a problem when the type of SCSI device dynamically changes, which can result in a kernel memory fault or memory inconsistency panic. This patch corrects a problem where interrupting an aseagent daemon with a signal can cause devices to become unaccessible. |
| Patch 1041.00<br>OSF445-440 | **Patch:** Problem with remote debugging of system kernel<br>**State:** New<br>This patch corrects a problem with remote debugging of a system kernel so that it is now possible with KDEBUG enabled. |
| Patch 1043.00<br>OSF445-383 | **Patch:** Savecore prematurely terminates crash dump recovery<br>**State:** New<br>This patch corrects a problem where savecore may prematurely terminate crash dump recovery on partitions larger than 4 GB. |
| Patch 1045.00<br>OSF445-250 | **Patch:** joind fails to clean up its lock files<br>**State:** Supersedes patch OSF445-168 (344.00)<br>This patch corrects the following:<br>• Corrects a problem with joind, which caused it to respond to certain client dhcp requests via the wrong port.<br>• Fixes a problem where joind may fail to clean up its lock files in /var/join. |

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

| | |
|---|---|
| Patch 1047.00<br>OSF445-486 | **Patch:** Corrects improper file or privilege management<br>**State:** New<br>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 1049.00<br>OSF445-576 | **Patch:** Fixes a problem with scu<br>**State:** New<br>This patch fixes a problem with scu where a mismatch between expected and found data displays incorrect data expected. |
| Patch 1051.00<br>OSF445-229 | **Patch:** Fix for fta driver<br>**State:** New<br>This patch corrects a problem with excessive receive overrun error messages from the fta driver. |
| Patch 1053.00<br>OSF445CDE-028 | **Patch:** CDE login screen truncates message in issue file<br>**State:** New<br>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 1064.00<br>OSF445-677 | **Patch:** genvmunix does not boot on system with Atalla AXL200<br>**State:** Supersedes Patch 52.00 (OSF445-047)<br>This patch corrects the following:<br>• Fixes a problem where genvmunix does not boot on a system with an Atalla AXL200 card installed.<br>• Fixes a problem that could generate a crash when running in lockmode 4. |
| Patch 1066.00<br>OSF445-674A | **Patch:** Security (SSRT2400)<br>**State:** New<br>This patch corrects the following:<br>• A potential security vulnerability has been discovered, where under certain circumstanes, system integrity may be compromised. HP has corrected this potential vulnerability.<br>• Updates BIND from V4.9.3 to 8.3.4. |

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

| | |
|---|---|
| Patch 1068.00<br>OSF445-674B | **Patch:** Security (SSRT0636U, SSRT2408, SSRT2410, SSRT2411, SSRT2400)<br>**State:** Supersedes patches OSF445-030 (34.00), OSF445-137 (276.00), OSF445-633 (688.00), OSF445-238 (690.00)<br>This patch corrects the following:<br>• 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.<br>• Fixes a problem of named producing a core file when named is started and the named.boot file has more than 32767 zones specified.<br>• 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.<br>• The following potential security vulnerabilities have been corrected:<br>SSRT2408 BIND - (Severity - High)<br>SSRT2410 BIND - (Severity - High)<br>SSRT2411 BIND - (Severity - High)<br>• 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.<br>• A potential security vulnerability has been discovered, where under certain circumstanes, system integrity may be compromised. HP has corrected this potential vulnerability.<br>• Updates BIND from V4.9.3 to 8.3.4. |
| Patch 1070.00<br>OSF445-676 | **Patch:** Fix for gated that causes core dump<br>**State:** New<br>This patch fixes a problem with gated where the daemon would dump core under certain circumstances. |
| Patch 1072.00<br>OSF445-681 | **Patch:** Security (SSRT3469, SSRT3531)<br>**State:** Supersedes patch OSF445-650 (1059.00)<br>• A potential security vulnerability has been identified in sendmail which may result in nonprivileged 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.<br>• 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.<br>SSRT3531 sendmail - (Severity - High) |

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

| | |
|---|---|
| Patch 1074.00<br>OSF445-683 | **Patch:** Revises reference pages for BIND update to V8.3.4<br>**State:** New<br>This patch revises the following reference pages for the update of BIND from V4.9.3 to V8.3.4:<br><br>named.boot.4.gz<br>named.conf.4.gz<br>named.star.4.gz<br>resolver.4.gz<br>bind_intro.7.gz<br>bind_manual_setup.7.gz<br>named-bootconf.8.gz<br>named-xfer.8.gz<br>named.8.gz<br>nslookup.8.gz |
| Patch 1079.00<br>OSF445-682 | **Patch:** Fix for newfs<br>**State:** Supersedes patch OSF445-154 (285.00)<br>This patch provides the following fixes:<br>• Signal parent process to enable user notification of mount failure.<br>• Return functionality to accept disk type from user.<br>• Exit if overlap detected and not being run interactively.<br>• Do not do check_usage for -N option or MFS.<br>• Move common variable declarations to header file.<br>• Adjust fssize and references to it to handle larger file systems.<br>• Corrects a problem with large file systems (> 16K cylinder groups) created by newfs/mkfs/extendfs, which can cause system panics when accessing data beyond cyl group 16K. |
| Patch 1081.00<br>OSF445-678 | **Patch:** Fixes a problem in rpc.lockd<br>**State:** Superseds patch 309.00 (OSF445-124)<br>This patch corrects the following:<br>• Fixes a problem in rpc.lockd where the FCNTL () function fails to lock NFS mounted directories.<br>• 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. |

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

| | |
|---|---|
| Patch 1083.00<br>OSF445-694 | **Patch:** System panics on configurations using Memory Channel<br>**State:** Supersedes patches OSF445-143 (319.00), OSF445-566 (975.00), OSF445-577 (976.00), OSF445-363 (977.00), OSF445-477 (978.00), OSF445-215 (980.00)<br>This patch corrects the following:<br>• Fixes a panic or a system hang which could occur on a DS20E with drives attached to the motherboard SCSI interface (Adaptec 7895-based) or on an Ultra3 KZPEA SCSI adapter. In addition to system hangs or panics on configurations using Memory Channel adapters, some configurations have exhibited SCSI device problems.<br>• Corrects problems in the aha_chim driver that could result in bus hangs, panics, and inappropriate access of freed memory during a high rate of bus resets.<br>• Incorrect I/O status may be returned by the KZPEA driver when attempting to abort an I/O during a reset.<br>• Fixes several problems found in the KZPEA driver that could result in hung I/O, pending I/O not being cleared on a reset, panics seen when abortng I/O, and hard error returned to applications on opens during reset conditions.<br>• CHIM changes to fix Ignore Wide Residue fix and Kernel Memory Fault panic.<br>• Fixes several problems found in the KZPEA driver that could result in memory corruption, bus hangs, and system panics. This patch also includes binary error logging support in the driver.<br>• KZPEA firmware fails to correctly handle filemarks with odd byte transfers. |
| Patch 1085.00<br>OSF445-697 | **Patch:** Fixes potential panic in auditing of swapctl syscall<br>**State:** New<br>This patch fixes a potential panic in the auditing of the swapctl syscall. |
| Patch 1087.00<br>OSF445-412C | **Patch:** Corrects improper file access<br>**State:** New<br>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 1093.00<br>OSF445-666 | **Patch:** rm -r command does not scale for large directories<br>**State:** New. Supersedes OSF445-623 (695.00)<br>This patch corrects the following:<br>• Addresses the performance issue of rm -r with large directories.<br>• Fixes the problem of a race condition in rm command, wherein two threads can successfully delete a file simultaneously. |
| Patch 1095.00<br>OSF445-679 | **Patch:** Fixes a potential problem in screend<br>**State:** New<br>This patch fixes a potential problem in screend. |

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

| | |
|---|---|
| Patch 1097.00<br>OSF445-672 | **Patch:** Fixes SDLT media error caused bus resets<br>**State:** Supersedes patches OSF445-081 (137.00), OSF445-211 (277.00), OSF445-192 (279.00), OSF445-345 (920.00), OSF445-527 (921.00), OSF445-402 (922.00), OSF445-254 (923.00), OSF445-528 (925.00)<br>This patch corrects the following:<br>• Fixes for the itpsa driver negotiating for ULTRA2 speed although the SCSI bus is single-ended.<br>• Fixes a problem that can cause a simple lock timeout or a kernel memory fault on EV6 systems using the itpsa driver.<br>• Fixes a problem with some slower tape devices serviced by the itpsa driver by lengthening the timeout value used.<br>• Fixes a kernel memory fault panic after an "ITPSA: itpsa_action - error converting path ID to ITPSA softc structure" message.<br>• Fixes a kernel memory fault related to the KZPCA adapter.<br>• Adds the capability for KZPCA devices to work with SCSI devices that only support asynchronous data transfers.<br>• 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.<br>• Fixes SDLT media error that caused bus resets with KZPCA adapters.<br>• Fixes a problem in the KZPCA itpsa driver that can be seen when a SCSI target presents multiple LUNs. |
| Patch 1099.00<br>OSF445-665 | **Patch:** Fixes a buffer overflow problem in usr/bin/write<br>**State:** New<br>This patch fixes a buffer overflow problem in /usr/bin/write. |
| Patch 1102.00<br>OSF445-713 | **Patch:** Enhancement to access control list functionality<br>**State:** New. Supersedes patches OSF445-315 (867.00), OSF445-706 (1100.00)<br>This patch corrects the following:<br>• 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 instead.<br>• If the ACL on a file is corrupted, the corrupted ACL is passed into the kernel causing a variety of problems.<br>• Fixes various problems in the ee driver for DE60x Ethernet adapters.<br>• Fixes an I/O hang condition on FibreChannel. |
| Patch 1103.00<br>OSF445-714 | **Patch:** Enhances SuperDLT maximum transfer size edit<br>**State:** New. Supersedes patches OSF445-531 (797.00), OSF445-446 (798.00), OSF445-546 (800.00)<br>This patch corrects the following:<br>• Changes the SuperDLT1 maximum transfer size.<br>• Provides device support for the SDLT160/320 tape drive.<br>• Enhances the SuperDLT maximum transfer size edit to be more tolerant of previous changes.<br>• Provides support for possible future Tape devices. |

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

| | |
|---|---|
| Patch 1105.00<br>OSF445-715 | **Patch:** Fixes unaligned kernel space access from km panic<br>**State:** Supersedes patch OSF445-140 (339.00)<br>This patch fixes a problem in which the system may panic with the panic string "Unaligned kernel space access from kernel mode". |
| Patch 1107.00 | **Patch:** (SSRT1-45U, SSRT2439, SSRT2341, SSRT0740U)<br>**State:** New. Supersedes patches OSF445-072 (79.00), OSF445-082 (138.00), OSF445-115 (140.00), OSF445-136 (281.00), OSF445-063 (67.00), OSF445-111 (130.00), OSF445-113 (192.00), OSF445-109 (201.00), OSF445-164 (250.00), OSF445-202 (251.00), OSF445-174 (252.00), OSF445-183 (253.00), OSF445-163 (255.00), OSF445-011 (16.00), OSF445-019 (24.00), OSF445-162 (262.00), OSF445-181 (264.00), OSF445-001 (14.00), OSF445-023 (81.00), OSF445-025 (29.00), OSF445-031 (35.00), OSF445-112A (91.00), OSF445-108 (93.00), OSF445-165 (208.00), OSF445-170 (209.00), OSF445-138 (211.00), OSF445-098 (105.00), OSF445-107 (122.00), OSF445-157 (266.00), OSF445-012 (17.00), OSF445-040 (45.00), OSF445-068 (71.00), OSF445-073 (78.00), OSF445-079 (75.00), OSF445-083 (176.00), OSF445-005 (55.00), OSF445-007 (73.00), OSF445-010 (15.00), OSF445-016 (21.00), OSF445-017 (22.00), OSF445-026 (30.00), OSF445-004 (44.00), OSF445-049 (54.00), OSF445-062 (66.00), OSF445-064 (68.00), OSF445-066 (69.00), OSF445-101 (108.00), OSF445-069 (72.00), OSF445-008 (74.00), OSF445-065 (141.00), OSF445-075 (142.00), OSF445-002 (143.00), OSF445-095 (110.00), OSF445-058A (145.00), OSF445-106 (114.00), OSF445-015 (20.00), OSF445-013 (18.00), OSF445-029 (32.00), OSF445-037 (41.00), OSF445-052 (57.00), OSF445-076 (107.00), OSF445-171 (212.00), OSF445-144 (213.00), OSF445-189 (214.00), OSF445-131 (215.00), OSF445-123 (216.00), OSF445-133 (217.00), OSF445-182 (218.00), OSF445-178 (219.00), OSF445-173A (220.00), OSF445-119 (221.00), OSF445-172 (222.00), OSF445-196 (223.00), OSF445-120 (224.00), OSF445-126 (225.00), OSF445-151 (226.00), OSF445-191 (227.00), OSF445-190 (228.00), OSF445-188 (229.00), OSF445-166 (230.00), OSF445-200 (231.00), OSF445-187 (232.00), OSF445-197 (233.00), OSF445-195 (235.00), OSF445-179 (236.00), OSF445-203 (237.00), OSF445-204 (238.00), OSF445-186 (240.00), OSF445-212A (348.00), OSF445-116 (303.00), OSF445-242 (356.00), OSF445-035 (39.00), OSF445-020 (25.00), OSF445-104 (170.00), OSF445-096 (172.00), |

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

| | |
|---|---|
| Patch 1107.00 continued | OSF445-046 (51.00), OSF445-085 (186.00), OSF445-039 (43.00), OSF445-158 (317.00), OSF445-102 (178.00), OSF445-139 (268.00), OSF445-067 (70.00), OSF445-053 (58.00), OSF445-510 (372.00), OSF445-367 (373.00), OSF445-308 (374.00), OSF445-272 (375.00), OSF445-334 (376.00), OSF445-506 (377.00), OSF445-598 (378.00), OSF445-377 (379.00), OSF445-494 (380.00), OSF445-378 (381.00), OSF445-634 (382.00), OSF445-352 (383.00), OSF445-516 (384.00), OSF445-595 (385.00), OSF445-504 (386.00), OSF445-274 (387.00), OSF445-517 (388.00), OSF445-294 (389.00), OSF445-309 (390.00), OSF445-423 (391.00), OSF445-210 (392.00), OSF445-433 (393.00), OSF445-602 (394.00), OSF445-269 (395.00), OSF445-426 (396.00), OSF445-224 (397.00), OSF445-630 (398.00), OSF445-364 (399.00), OSF445-459 (400.00), OSF445-513 (401.00), OSF445-591 (402.00), OSF445-484 (403.00), OSF445-327 (404.00), OSF445-227 (405.00), OSF445-360 (406.00), OSF445-500 (407.00), OSF445-523 (408.00), OSF445-340 (409.00), OSF445-393 (410.00), OSF445-406 (411.00), OSF445-316 (412.00), OSF445-235 (413.00), OSF445-411 (414.00), OSF445-244 (415.00), OSF445-476 (416.00), OSF445-425 (417.00), OSF445-321 (418.00), OSF445-324 (419.00), OSF445-545 (420.00), OSF445-462 (421.00), OSF445-317 (422.00), OSF445-464 (423.00), OSF445-524 (424.00), OSF445-313 (425.00), OSF445-398 (426.00), OSF445-263 (427.00), OSF445-458 (428.00), OSF445-619 (429.00), OSF445-607 (430.00), OSF445-508 (431.00), OSF445-501 (432.00), OSF445-332 (433.00), OSF445-530 (434.00), OSF445-300 (435.00), OSF445-468 (436.00), OSF445-471 (437.00), OSF445-351 (438.00), OSF445-639 (439.00), OSF445-621 (440.00), OSF445-374 (441.00), OSF445-231 (442.00), OSF445-312 (443.00), OSF445-350A (444.00), OSF445-291 (445.00), OSF445-442 (446.00), OSF445-381 (447.00), OSF445-529 (448.00), OSF445-222 (449.00), OSF445-356 (450.00), OSF445-275 (451.00), OSF445-358 (452.00), OSF445-436A (453.00), OSF445-379 (454.00), OSF445-281 (455.00), OSF445-283 (456.00), OSF445-283 (456.00), OSF445-368 (457.00), OSF445-279 (458.00), OSF445-437 (459.00), OSF445-586 (460.00), OSF445-495 (461.00), OSF445-266 (462.00), OSF445-209 (463.00), OSF445-336 (464.00), OSF445-485 (465.00), OSF445-490 (466.00), OSF445-434 (467.00), OSF445-292 (468.00), OSF445-400 (469.00), OSF445-625 (470.00), OSF445-463 (471.00), OSF445-299 (472.00), OSF445-262 (473.00), OSF445-355 (474.00), OSF445-534 (475.00), OSF445-636 (476.00), OSF445-349 (477.00), OSF445-306 (478.00), OSF445-386 (479.00), OSF445-218 (480.00), OSF445-574 (481.00), OSF445-503A (482.00), OSF445-370 (483.00), OSF445-342 (484.00), OSF445-304 (485.00), OSF445-582 (486.00), OSF445-543 (487.00), OSF445-438 (488.00), OSF445-637 (489.00), OSF445-216 (490.00), OSF445-536 (491.00), OSF445-416 (492.00), OSF445-335 (493.00), OSF445-314 (494.00), OSF445-225 (495.00), OSF445-385 (496.00), OSF445-427 (497.00), OSF445-318 (498.00), OSF445-301 (499.00), OSF445-236 (500.00), OSF445-237 (501.00), OSF445-472 (502.00), OSF445-600 (503.00), OSF445-373 (504.00), OSF445-430 (505.00), OSF445-290 (506.00), OSF445-257 (507.00), OSF445-375 (508.00), OSF445-415 (509.00), OSF445-232 (510.00), OSF445-248 (511.00), OSF445-596 (512.00), OSF445-554 (513.00), OSF445-219A (514.00), OSF445-357 (515.00), OSF445-479 (516.00), |

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

| | |
|---|---|
| Patch 1107.00 continued | OSF445-247 (517.00), OSF445-325 (518.00), OSF445-208 (519.00), OSF445-457 (520.00), OSF445-303 (521.00), OSF445-401 (522.00), OSF445-330 (523.00), OSF445-541 (524.00), OSF445-618A (525.00), OSF445-564A (526.00), OSF445-544 (527.00), OSF445-573 (528.00), OSF445-441 (529.00), OSF445-320 (530.00), OSF445-273 (531.00), OSF445-409 (532.00), OSF445-444 (533.00), OSF445-333 (534.00), OSF445-392 (535.00), OSF445-456 (536.00), OSF445-443 (537.00), OSF445-289 (538.00), OSF445-572 (539.00), OSF445-261 (540.00), OSF445-410 (541.00), OSF445-293 (542.00), OSF445-532 (543.00), OSF445-220 (544.00), OSF445-655 (545.00), OSF445-505 (546.00), OSF445-606 (547.00), OSF445-418 (548.00), OSF445-481A (549.00), OSF445-341 (550.00), OSF445-585 (551.00), OSF445-514 (552.00), OSF445-407 (553.00), OSF445-353 (554.00), OSF445-339 (555.00), OSF445-258 (556.00), OSF445-412A (557.00), OSF445-276 (558.00), OSF445-535 (559.00), OSF445-344 (560.00), OSF445-284 (561.00), OSF445-461 (562.00), OSF445-469 (563.00), OSF445-626A (564.00), OSF445-649 (565.00), OSF445-552 (566.00), OSF445-466 (567.00), OSF445-282 (568.00), OSF445-453 (569.00), OSF445-286 (570.00), OSF445-496 (571.00), OSF445-361 (572.00), OSF445-285 (573.00), OSF445-297 (574.00), OSF445-647 (575.00), OSF445-278 (576.00), OSF445-454 (577.00), OSF445-624 (578.00), OSF445-509 (579.00), OSF445-395 (580.00), OSF445-337 (581.00), OSF445-277 (582.00), OSF445-223 (583.00), OSF445-643 (584.00), OSF445-372 (585.00), OSF445-535 (559.00), OSF445-344 (560.00), OSF445-284 (561.00), OSF445-461 (562.00), OSF445-469 (563.00), OSF445-626A (564.00), OSF445-649 (565.00), OSF445-552 (566.00), OSF445-466 (567.00), OSF445-282 (568.00), OSF445-453 (569.00), OSF445-286 (570.00), OSF445-496 (571.00), OSF445-361 (572.00), OSF445-285 (573.00), OSF445-297 (574.00), OSF445-647 (575.00), OSF445-278 (576.00), OSF445-454 (577.00), OSF445-624 (578.00), OSF445-509 (579.00), OSF445-395 (580.00), OSF445-337 (581.00), OSF445-277 (582.00), OSF445-223 (583.00), OSF445-643 (584.00), OSF445-372 (585.00), 1057.00 (OSF445-614), OSF445-675 (1060.00), OSF445-648 (1062.00), OSF445-692 (1075.00), OSF445-695 (1077.00), OSF445-700 (1088.00), OSF445-651 (1089.00), OSF445-654 (1091.00), OSF445-315 (867.00), OSF445-706 (1101.00)<br>This patch corrects the following:<br>• 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.<br>• Fixes a printing problem where 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 two-second timeout which may cause a job-submit failure on the job-number wraparound. |

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

| | |
|---|---|
| Patch 1107.00 continued | • A user is unable to delete a print job from a remote system with a host name greater than 32 characters because the host name was truncated.<br>• When a TCP/IP connection fails, the retry algorithm would take longer to print jobs due to a long retry interval.<br>• A timing hole during lpd last-job completion and shutdown needed to be closed.<br>• It was not possible to print to the lpd queue using Windows 2000.<br>• Corrects a problem in which, under certain conditions, unnecessary error messages are written to the lpr.log file.<br>• 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/IF connection for each job in the print queue (JJ=0). It also closes a timing hole that existed when lpd was shutting down.<br>• Fixes a problem in which lpd hangs when printing to advanced server queues (using /dev/null).<br>• Updates the emx Fibre Channel driver to Revision 1.22, correcting a successive command timeout problem. This error would cause degraded performance.<br>• This patch fixes the following DE600/DE602 10/100 Ethernet adapters problems:<br>– The primary CPU may appear hung on networks where switches send "Flow Control Pause" frames if they become overloaded.<br>– Transmit timeout messages appear in the console log due to the driver timing out a frame.<br>– Provides the device driver support for the 3DLabs Oxygen VX1 graphics adapter.<br>– Provides support for the DEGPA-TA (1000BaseT) Gigabit Ethernet device.<br>• Fixes a "u_anon_free: page busy" panic.<br>• 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.<br>• Fixes an issue with lightweight wiring of pages and shared memory regions.<br>• Fixes a problem where cascaded switches can hang the system at failover time.<br>• Addresses two problems with the ee driver for DE60x Ethernet cards. These problems affect all Tru64 systems containing ee cards.<br>– Fixes a race condition where the card could stop receiving packets from the network under rare circumstances.<br>– Fixes for the lan_config user options -x and -s. |

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

| | |
|---|---|
| Patch 1107.00 continued | • Fixes a problem in ksh. When the current working directory is / and the command cd .. is entered, the following error message is displayed:<br><br>ksh: ..: bad directory<br><br>• Fixes a problem in ksh in which a space after the -p option would cause the command to fail.<br>• Fixes a possible handling problem with multibyte character boundary conditions in ksh script processing.<br>• Fixes two ksh problems that occur in multibyte Asian locales.<br>• Adds a NULL to the resulting string output of swprintf() calls.<br>• Fixes a problem in libc that affects debugger tracebacks of code containing split procedures.<br>• Fixes a problem where gmtime() was erroneously setting the tzname[0] array.<br>• Increases the length of the user names for rsh and rexec to allow for NT interoperabilty.<br>• Addresses performance and scalability issues for highly contended threaded applications running on EV6 SMP machines.<br>• Fixes a problem for those applications that assume that initial allocations of memory from the C run-time library's malloc() function will return only zero-filled memory.<br>• Fixes a problem that might occur with threaded applications linked against older versions of DECthreads. The DECthreads internal symbol __pthreads_legacy_init_routine may show up as an unresolved symbol at load time when those applications are run on systems on which a newer version of DECthreads has been installed.<br>• 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.<br>• Prevents "not currently mounted" warning messages from being displayed for file systems the user did not request to umount.<br>• Upgrades the sys_check utility to Version 119.1 and provides the following changes:<br>– Fixes the ra200info tool from core dumping.<br>– Utilizes Compaq Analyze when available.<br>– Utilizes storage's new cliscript tool in place of hszterm.<br>– Updates ASU section.<br>– Fixes two NFS problems.<br>• Upgrades the sys_check utility to Version 120.<br>• 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.<br>• Fixes a system hang that could last up to a few minutes with large files when performing synchronous I/O requests and a flushing loop.<br>• Fixes a problem where, in the output of a ps command, the PAGEIN column reports 0 for all processes.<br>• Patch turns off AdvFS assert which, when turned on, a performance degradation in AdvFS occurs. |

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

| | |
|---|---|
| Patch 1107.00 continued | • 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.<br>• Fixes a problem with AdvFS. An AdvFS domain becomes inaccessible when using the mount -d option.<br>• Fixes a kernel memory fault in VMAC code if_addnewaddr().<br>• Adds a fix to VMAC functionality when used with NetRAIN.<br>• Fixes a problem where the following can occur during a system panic:<br>– System calls interrupts<br>– mpsleep() returns an EINTR error when the panicstr is non-NULL<br>– An infinite looping at a very high priority<br>• 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.<br>• Fixes a problem in which operations on NFS files can hang indefinitely.<br>• Fixes a problem that causes corruption in the floating point registers whereby the flag fields nxm_fp_owned are overwritten with 0s.<br>• 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.<br>• Fixes a system panic with the panic string:<br>psig: catch not set<br>• 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.<br>• Fixes a problem in which the POSIX interval timer is not resilent to clock slowdown caused either by NTP or by a backwards change of the clock.<br>• Fixes a kernel memory fault seen under certain conditions when setting a thread's priority.<br>• 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. This patch corrects the problem.<br>• This patch fixes two panics that have the following error messages:<br>simple_lock: time limit exceeded<br>simple_lock: lock already owned by cpu<br>• Corrects a problem with the incorrect ordering of network interfaces which was resulting in network partitions.<br>• Fixes a panic associated with ASE service failover.<br>• Fixes a panic in in_pcbfree() when NFS is implemented over TCP.<br>• Fixes a problem with relocating an TCR/ASE NFS service when one or many clients have the service mounted over TCP.<br>• Coding change to ip_insertoptions() to correct excessive execution time in routine in_cksum due to invalid message length. |

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

| | |
|---|---|
| Patch 1107.00 continued | • Fixes reply values for NFS writes which were causing protocol violations.<br>• Prevents a possible NFS over TCP hang. NFS TCP threads will be blocked in sosbwait() causing the system to appear to hang.<br>• Fixes a problem where the operating system only looks in slot 0 for the primary CPU.<br>• 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.<br>• Fixes a simple_lock time limit exceeded panic due to an SMP race condition in namecache.<br>• Fixes a race condition in the UBC code where a lookup is done on a page being invalidated (freed).<br>• Includes UFS delayed metadata mount option that fixes metadata-intensive application performance.<br>• Fixes a hang or simple_lock_state_violation panic in biodone.<br>• 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.<br>• 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.<br>• Fixes panics which can occur if a signal is sent to a multithreaded task in which one or more threads are calling exit() or exec().<br>• Fixes a problem in which the wrong status was returned from EEROM read.<br>• Corrects a problem where a directory entry may be attempted to be changed to "." and the code checks for this prevents it from happening.<br>• Fixes a panic in AdvFS which has the following error message:<br>panic: Unaligned kernel space access from kernel mode.<br>• 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.<br>• 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.<br>• Provides support for activating temporary data logging on a mount point.<br>• Fixes a kernel memory fault from ufs_mount().<br>• 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().<br>• Corrects a simple lock timeout seen when dealing with NFS loopback mounted file systems with large amount of dirty pages. |

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

| | |
|---|---|
| Patch 1107.00 continued | • Prevents a system panic from occurring while using AdvFS.<br>• Fixes a "simple_lock: time limit exceeded" system panic either from cache_lookup() or cache_enter(). This is caused by the namecache LRU list getting corrupted.<br>• Fixes inaccuracy problems when using setrlimit/getrlimit with a threaded application.<br>• Fixes a hang in the UFS file system.<br>• Fixes a memory leak when named pipes (FIFOs) are used.<br>• Fixes a problem that causes Tarantella Enterprise 1.41 not to install on Tru64 UNIX.<br>• CDFS media burned in 2001 shows the wrong dates.<br>• 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.<br>• Fixes a problem where threads can hang in x_load_in-mem_xtnt_map().<br>• Fixes a potential problem flushing data to disk when using data logging with sparse files.<br>• Corrects an AdvFS panic which can occur during a rmfset operation with the panic string: "rbf_delete_int: can't find bf attributes".<br>• 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.<br>• Fixes a problem when using multiple subnets on a network interface; ARP 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.<br>• Fixes a problem when applications make IOCTL calls using an IP alias address on a network interface.<br>• Modifies AdvFS kernel code and several utilities. AdvFS will no longer panic with the following error:<br>`ADVFS EXCEPTION : panic cpu(0) : bad frag free list`<br>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. |

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

| | |
|---|---|
| Patch 1107.00 continued | • Fixes two problems with the consvar command:<br>– consvar -s now sets a tape device as a boot device from the console.<br>– consvar -g now displays a listing of the console settings as intended.<br>• Fixes a "simple_unlock: lock not owned by cpu" panic in the biodone routine.<br>• Fixes a problem of NetRAIN devices failing to come up after the rcinet restart command is entered.<br>• An invalid error message when attempting to move files in which the source name is the same as the destination name.<br>• When using mv -i to rename a symlink pointing to a file on a different filesystem owned by a different user, this results in the prompt:<br>Ownership of y will change. Continue?<br>• When moving a file from one file system to another, the mv command will copy the file rather than using the rename() system call, which can result in file loss.<br>• Corrects the problem with the mv(1) command deleting files in the directory when the user moves a directory to itself.<br>• Fixes a problem where some crontab jobs would run multiple times in the same minute.<br>• The cron daemon does intensive logging and fills up the disk.<br>• 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.<br>• 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.<br>• Corrects a problem that occurred when routine pmap_coproc_exit_notify() modifies the pmaps' coproc_tbi function to be 0, a null pointer, when it was being checked by routine pmap_remove_all().<br>• Fixes a problem in which the vi editor core dumps when it finds invalid syntax during a substitute operation.<br>• Fixes a problem in the what command, where it was unable to process more than one input file at once.<br>• Fixes several problems when bindsetup is used to change host names.<br>• Fixes three problems in dbx:<br>– dbx stack trace is incomplete.<br>– Assignment to a variable would fail after viewing a nonlocal symbol.<br>– The use of vfork would raise a signal 66. |

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

| | |
|---|---|
| Patch 1107.00 continued | • Fixes a problem with btcreate command where default restore fails if the disklabel is different. This patch also fixes a btextract character missing problem and extends the robot media changer sleep time for slower media changers.<br>• 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.<br>• Fixes two possible panics in AdvFS:<br>– One caused by bs_real_invalidate_pages.<br>– One caused by bs_purge_dirty.<br>• Fixes a kernel memory fault due to a bug in kernel code.<br>• Corrects a problem with ICMP redirect processing which resulted in incorrect ICMP redirect messages.<br>• Addresses a kernel memory fault panic in malloc_thread().<br>• 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.<br>• Fixes a problem where memory could retain execute permission on EV6 machines.<br>• Fixes a delete_pv_entry panic when kernel virtual address space has high usage.<br>• Corrects a problem where df was showing negative values for large NFS file systems.<br>• Corrects a problem introduced in a prior patch which can result in a system panic when outputting through the packet filter.<br>• To avoid log inconsistencies we no longer reuse log pages. In one case these inconsistencies resulted in a system hang caused by a huge, unreasonable malloc.<br>• 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".<br>• 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.<br>• Shell inline input files are more secure.<br>• sh noclobber and new constructs were added.<br>• 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 1107.00 continued | • Fixes problem that occurred 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.<br>• Corrects problems of audit_tool supplying incorrect or insufficient data about an audit event.<br>• Corrects two problems:<br>– The table() system will not abort connections properly if a tcb hash table number is greater than 1.<br>– 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.<br>• Fixes two code paths where the user could accidentally look up 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.<br>• Prevents a race in msfs_umount.<br>• 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.<br>• Fixes kernel memory faults caused by ufs_sync_int accessing an inactivated or deallocated vnode.<br>• 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.<br>• 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.<br>• Fixes a ksh problem related to cleaning the process when the terminal is abruptly stopped.<br>• 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.<br>• Prevents a possible lock hierarchy violation while opening a clone.<br>• Fixes a kernel memory fault that can occur after a user issues "kill-STOP".<br>• Addresses three issues:<br>– The TCP window has been increased from 96 KB to 500 KB for performance improvements.<br>– This patch will have the netisr thread dynamically estimate the reply size and subsequently reserve the space in the socket buffer.<br>– 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.<br>• Fixes a problem where decreasing the smoothsync_age does not always have an effect. |

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

| | |
|---|---|
| Patch 1107.00 continued | • 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.<br>• Corrects a problem with could result either in the panic of a cluster member or in inconsistent data when the sbcompress_threshold configurable is set.<br>• 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.<br>• The following potential security vulnerability has been corrected: SSRT2384 RPC (Severity - High)<br>• Prevents the error message "local HSM Error: msgsvc: socket close failed" from being generated when an application closes the socket with return state 0.<br>• Updates the emx driver to v2.03 and fixes a problem which could cause an emx driver panic during adapter resets.<br>• Installs DECthreads V3.16-032, which fixes problems that may effect threaded programs using pthread_kill() on Tru64 UNIX V4.0G systems.<br>• Fixes the kernel memory fault panic in the IP multicast loopback code.<br>• Corrects a problem with the counters maintained for the NetRAIN virtual interface.<br>• 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.<br>• Corrects a problem in which ksh did not clean up the processes associated with a terminal once the window was closed.<br>• Fixes a problem which can result in a panic, hang, or inconsistencies from vnode deallocation during an unmount. This also fixes a “VFS_UNMOUNT panic” upon unmount.<br>• Fixes a panic with simple_lock_timeout due to too many pages to scan in ubc_page_alloc().<br>• Fixes heap and stack limitations in the older operating system. versions required for SAP.<br>• Avoids 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.<br>• A potential security vulnerability has been discovered where, under certain circumstances, system integrity may be comprimised when a buffer overflow occurs in the ypmatch and traceroute utilities. Buffer overflows are sometimes exploited in an attempt to subvert the funcuion 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.<br>• Prevents a panic in fifo_write with the panic message "NULL fifo_bufhdr append pointer".<br>• Fixes a problem that causes a system panic when a program calls sendfile(2) to access a file via NFS. |

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

| | |
|---|---|
| Patch 1107.00 continued | • Corrects a problem found where the rmtmpfiles script would produce errors at startup of the form:<br><br>dirclean: lstat failure for starting directory: /.osonly_tmp/:<br>No such file or directory<br><br>• Fixes an application core dump problem when the LANG environment variable is too long.<br><br>• 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.<br><br>• Fixes sync-related processing of vnodes in AdvFS and NFS.<br><br>• Fixes a "kernel memory fault" panic in the Virtual Memory subsystem on SMP systems.<br><br>• Fixes a regular expression performance problem in sed.<br><br>• A potential security vulnerability has been discovered in the kernel where, under certain circumstances a race condition can occur that could allow a nonroot user to modify any file and possibly gain root access.<br><br>• Eliminates a false directory lookup warning message generated by an incorrect comparison caused by mismatched file id variable types. The fix also slightly improves client caching performance.<br><br>• 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.<br><br>• sh now prints the correct message when enhanced core file naming is on.<br><br>• Resolves kernel memory faults in the TCP/IP subsystem.<br><br>• Corrects the problem where telnetd leaves an extra UDP port open.<br><br>• Fixes mbuf memory corruption that can cause kernel memory fault panics.<br><br>• Resolves a problem of not being able to view files on some CD-ROM media that is created by third-party software.<br><br>• Fixes locking on retry case for multithreaded select/poll. A panic with the stack trace “PANIC: thread_block: simple lock owned” is indicative of this problem:<br><br>• 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.<br><br>• Fixes the following problems in sh:<br><br>– Service denial problem when a quoted here doc script is executed.<br><br>– Problem with handling ELF files.<br><br>– The shell variable $- not holding -C set option when it is turned on.<br><br>– Printing broken characters when type builtin utility of sh is invoked in Japanese locale. |

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

| | |
|---|---|
| Patch 1107.00 continued | • 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).<br>• Installs DECthreads V3.16-030, which fixes problems that may affect threaded programs which use the fork() system call running on Tru64 UNIX V4.0G.<br>• Fixes the following editors to handle tags functionality using the <Ctrl/T> key:<br>– vi<br>– edit<br>– ex<br>– view<br>– vedit<br>• Fixes a problem with ksh. When a ksh menu is started from within a user's .profile, ksh will not stop when the telnet session is stopped.<br>• Correction in cron to correctly handle backslash (\) commands so that crontab and /dev/console output do not include backslashes.<br>• 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.<br>• Avoids a domain panic when a E_CANT_ACCESS_LOG error is detected.<br>• Corrects a problem where offlining a CPU with bound process(es) can lead to a "malloc_check_checksum: memory pool corruption" panic.<br>• Fixes a problem that affects threaded programs compiled with the taso option on Tru64 UNIX V4.0G. The default stack size for taso user threads in DECthreads V3.16 was too large.<br>• 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:<br>– A fix for vMAC support. Prior to this patch, vMAC has not worked with DEGPA.<br>– A fix to prevent two DEGPA adapters from getting the same MAC address in a NetRAIN configuration.<br>• Fixes a rare panic in the driver for the DE600/DE602 10/100 Ethernet adapter.<br>• Fixes a problem where a system crash occurs at the end of a rmvol. The following panic string will be seen:<br>panic (cpu 0): lsn_io_list: current lsn > hiflushlsn<br>• Fixes system panic and/or data inconsistencies caused by changing fifo parameter pipe-databuf-size while fifo operations are in flight.<br>• Fixes a bug that causes inconsistencies in binary.errlog.<br>• Eliminates a "Simple Lock Time Limit Exceeded" due to the IoQueueMutex being held in bs_real_invalidate_pages.<br>• Fixes a problem with multi-threaded applications that can cause the application to consume 100% of the CPU usage time.<br>• Fixes an lpd problem, a memory leak associated with the allocation of a buffer. |

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

| | |
|---|---|
| Patch 1107.00 continued | • Fixes a problem in the VM subsystem that could cause a crash with the panic string "vm_page_ssm_unwire".<br>• Prevents segmentation faults when sia_ses_init is passed a malformed argument vector.<br>• 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.<br>• Provides the /usr/lbin/mkstemp program which allows the mechanism to create a secure temporary file.<br>• Resolves a problem in which there was a panic (“simple lock: time limit exceeded”) in spec_reclaim.<br>• Provides fuser functionality to allow detecting unlinked referenced files.<br>• 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.<br>• 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.<br>• The following potential security vulnerability has been corrected:<br>SSRT2301 uudecode (Severity - Medium)<br>• 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.<br>• Fixes a problem in fwrite() where it was failing when the total number of bytes to be written is larger than 2 GB.<br>• Fixes performance shortcomings in NXM thread replacement.<br>• Eliminates the compiler warnings in ksh.<br>• A potential security vulnerability has been identified in the HP Tru64 UNIX operating system which may result in nonprivileged 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.<br>• The following potential security vulnerability has been corrected:<br>SSRT0845U stdio file descriptors (Severity - High)<br>• Corrects a problem where the SNMP interface counter ifInUcastPkts occassionally decrements or jumps to an arbitrary, large value. |

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

| | |
|---|---|
| Patch 1107.00 continued | • Updates the emx driver to V2.01 and fixes the following problems:<br>– A problem of unexpected tape I/O aborts.<br>– A panic of "Can't grow probe list".<br>– Several kernel memory faults within the driver.<br>– Redundant adapter failures no longer panic the system.<br>– A problem of panicing with low memory resources.<br>– Stalling I/O during reprobing when a cluster member goes down.<br>• Fixes a segmentation fault problem with long LOCPATH and LANG values.<br>• Systems configured with VX1 graphics card will not return to the console when the halt button is pressed. The console is then unusable.<br>• Eliminates compiler warnings in ksh.<br>• Fixes a problem with strerror where buffers could not be allocated.<br>• Fixes a problem with malloc() over-allocating memory from the kernel when malloc tuning variable __sbrk_override has been set to 1.<br>• Fixes a kernel panic with "get_xm_page_range_info:kernel memory fault".<br>• Fixes an occasional panic that can be seen when reading from a process using Granularity Hints via procfs.<br>• 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.<br>• Fixes a problem with vm_faults against anon objects mapped by multiple map entries.<br>• Corrects the problem where the DLI queue stalls when there is no traffic in the TCP/IP or HDLC stacks.<br>• When the file system is full, now crontab will not be removing its entries and vi also will not be truncating the existing file.<br>• Corrects the problem where a user may experience a core dump, when using csh from the Japanese locale.<br>• Fixes excessive FIDS_LOCK contention observed when large numbers of files are using system-based file locking.<br>• Enhances cron to now do extensive logging.<br>• 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.<br>• Fixes a problem in the kernel network subsystem that caused a kernel memory fault panic in the routine m_adj().<br>• Addresses three problems with the ee driver for DE60x Ethernet cards. These problems affect all Tru64 systems containing ee cards.<br>– Fixes a race condition where the card could stop receiving packets from the network under rare circumstances.<br>– Improves error checking when allocating buffers.<br>– Fixes DMA resource allocation to prevent a panic when a machine runs low on DMA resources. |

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

| | |
|---|---|
| Patch 1107.00 continued | • Fixes a problem with fopen. fopen was returning "file not found" when there was insufficient memory to allocate the file structure. fopen now returns "not enough space" for this case.<br>• Fixes a bug that could cause a panic with the panic string "ubc_object_free: page still resident".<br>• 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.<br>• Corrects a possible panic when auditing execve with exec_argp/exec_envp enabled.<br>• 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.<br>• Fixes locking problems in vclean().<br>• In u_anon_dupu(), the error-handling path at label pg_error should remove the entries that have been made in the physical map.<br>• Fixes a problem where network interfaces can appear unresponsive to network traffic.<br>• 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.<br>• The /usr/sbin/dirclean utility no longer attempts to remove the AdvFS .tags directory or the quota.group and quota.user files.<br>• Fixes a problem with booting over the network (dataless management) and booting from a tape device.<br>• Corrects two problems:<br>– New_wire_method (light weight wiring) issues known as the Oracle connect problem or Oracle performance problem.<br>– ARMTech kernel malloc invalid size panic.<br>• Fixes an Asian language processing problem under the Korn shell.<br>• Corrects a problem in the virtual file system that could cause a panic with the panic string "kernel memory fault."<br>• Corrects a problem in the virtual file system that could cause panic with the panic string "kernel memory fault."<br>• Allows fuser to display the reference flag. This option indicates the type of reference made. For example: open, closed, unlinked, or mmapped. |

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

| | |
|---|---|
| Patch 1107.00 continued | • Fixes a problem in which lpd hangs when printing to advanced server queues (using /dev/null).<br>• Fixes a bug that can cause a panic when a system is powering down.<br>• ARP request for a permanent ARP entry is ignored, and the user cannot connect from remote system.<br>• Corrects an lpc regression in the lpc buffer overflow fix.<br>• Corrects an AdvFS problem where an on-disk variable wraps when more than 64 K 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.<br>• 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 commnads. Buffer overflows are sometimes exploited in an attempt to subvert the function of a privileged program and possibly execute commnads and the elevated privileges if the program file has the setuid privilege. HP has corrected this potential vulnerability.<br>• Fixes a problem in which /usr/bin/ksh hangs for certain scripts that contain wait(1).<br>• Fixes an "unaligned access" panic when attempting to free or malloc memory from the 512-byte kernel memory bucket (bucket 5).<br>• Fixes a problem with AdvFS where mounting the file system with option -o dual causes a panic.<br>• Fixes segmentation errors that can occur when running SAS.<br>• 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.<br>• Corrects a problem in which sh was using a high amount of CPU time.<br>• Corrects a race condition which could result in a failure to set the modification time of a file. This occurs only on a UFS filesystem.<br>• Fixes the audit_tool search algorithm to differentiate between prived and non-prived uids, and to allow requlars expressions in string searches.<br>• 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.<br>• Fixes a problem with audit data not being displayed by the audit tool, problems with file object selection/deselection and directories, and NUMA performance issues associated with auditing.<br>• Prevents panics caused by bad arguments to system calls.<br>• 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.<br>• The following potential vulnerability has been corrected:<br>SSRT2322 - BIND resolver (Severity - High) |

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

| | |
|---|---|
| Patch 1107.00 continued | • Improves msync performance on files that are mapped with the MAP_PRIVATE flag.<br>• 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.<br>• 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".<br>• Fixes a problem that caused the 4.3BSD socket interface to return incorrect values for IOCTL calls accessing IP alias address information.<br>• 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.<br>• Fixes numerous problems of accessing deallocated and freed vnodes.<br>• Fixes an ISO9660 file system size limitation of 2.1 GB and provides full capacity access to DVD-ROM media.<br>• Prevents USB from initializing on systems where USB is not supported.<br>• 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.<br>• Fixes a problem when there is a hole in the virtual disk array.<br>• Provides a new lpd to fix /etc/hosts.lpd case sensitivity. For example, node.domain is treated the same as Node.Domain.<br>• Corrects the problem of a simple lock timeout due to POSIX timers and also corrects some inaccuracies of the POSIX realtime timers.<br>• 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.<br>• 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).<br>• Corrects a potential system hang when the directory link limit is reached while creating subdirectories. This patch also corrects the erroneous reporting of success when attempting to write beyond the file size limit using synchronized I/O.<br>• Corrects a problem where an fcntl() with the FIFO parameter would return errno=22 (Invalid Argument).<br>• Fixes a problem caused when the Tru64 UNIX TCP layer prematurely closes a slow but good connection with TCP reset.<br>• 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 1107.00 continued | • The return value of unlink() call was not checked when two threads were trying to move a file to two different destinations. Due to this, though one of the threads could unlink() the source file, there were no relevant error message displayed. A fix is given to address this issue.<br>• Corrects u_anon_free: page busy panics.<br>• 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.<br>• 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.<br>• Contains a fix for a Tru64 UNIX NFS server panic caused by receiving illegal file access mode from an NFS client.<br>• 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.<br>• The following potential security vulnerability has been corrected:<br>SSRT2266 IGMP (Severity - High)<br>• 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.<br>• 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.<br>• Fixes a kernel memory fault in msg_rpc_trap.<br>• Fixes a system panic resulting from a rare race condition. The panic error message is “kernel memory fault”.<br>• Corrects the problem of a rexec command hanging on a system.<br>•<br>• Fixes a problem of incorrect default route modification in which there is a race condition between gated startup and installation of static routes.<br>• Fixes a potential security problem.<br>• Fixes two problems in the ee driver for DE60x 10/100 Ethernet adapters. These problems affect all Tru64 UNIX systems containing DE60x network interfaces.<br>• 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.<br>• Makes start up scripts in /sbin/init.d world readable.<br>• Fixes sh problem while executing here document through command substitution. |

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

| | |
|---|---|
| Patch 1107.00 continued | • 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.<br>• 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.<br>• Fixes a problem with the c shell (csh) so that it now correctly recognizes the backslash (\) meta character.<br>• 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.<br>• A potential security vulnerability has been discovered in networking where, under certain circumstances, an alias IP address could be incorrectly promoted to being the primary address when another alias is removed. A remote system can take over packets destined for another host.<br>• Corrects a problem which could result in an alias IP address being incorrectly promoted to being the primary address when another alias is removed.<br>• Fixes a problem where a system can panic with a kernel memory fault in malloc.<br>• Corrects a problem with csh(1) where, if a non-root user performed an ls(1) with wildcard 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".<br>• Corrects an NFS hang when the delayed option is used with the mount command.<br>• A potential security vulnerability has been identified in the HP Tru64 UNIX operating system which may result in nonprivileged 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.<br>• Fixes a problem that sometimes caused the system to select the incorrect IP source address for outgoing connections when using IP aliases and subnetting on a network interface.<br>• Fixes three problems with the alt driver for DEGPA Gigabit Ethernet adapters. These problems affect all Tru64 UNIX systems containing DEGPA network interfaces.<br>• Improper scheduling of cron jobs related to months not having 31 days is now corrected. |

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

| | |
|---|---|
| Patch 1107.00 continued | • 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.<br>• Fixes a problem resulting in a system panic for applications that directly call nxm_get_bindings.<br>• Fixes a potential problem where system responsiveness may be impacted.<br>• Fixes a system panic with the 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.<br>• Corrects a kernel memory fault panic in clntktcp_connect().<br>• Fixes a problem in audit_tool which appends nonsense characters to the audit information to the output of an execve event in brief mode.<br>• A potential security vulnerability has been discovere, 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.<br>• Fixes a memory leak when using dlclose in libraries in a threaded application.<br>• Fixes the predictable TCP Sequence Number.<br>• Fixes memory leaks caused by certain type of scripts which is called in infinite loop. This consumes more virtual address space over time.<br>• sh will not receive SIGSEGV signal when you run type with file path > 69 chars.<br>• 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.<br>• Corrects a problem in audit_tool parsing the n, p, or u options of the -a, -u, or -r switches and corrects the audit_tool usage message to reflect current funtionality.<br>• 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.<br>• The following potential security vulnerability has been corrected:<br>SSRT2266 IGMP (Severity - High)<br>• Fixes an assert_wait panic coming from k_mem_fault.<br>• The gettimezone script fails to present menus properly.<br>• 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.<br>• Fixes the problem of /usr/bin/csh picking the wrong message catalog entry from the translated message catalog when LANG was set to Japanese locale. |

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

| | |
|---|---|
| Patch 1107.00 continued | • Fixes a problem in the Network startup script where it could fail to configure an interface with an IP address.<br>• Corrects possible security hole reported by SSRT2323.<br>• Fixes the problem encountered with the Bourne shell when a file name with trailing slash (/) is used as an argument to the command.<br>• NIS clients may fail to connect to non-Tru64 UNIX NIS servers that only support the V2 NIS protocol.<br>• Fixes a problem where, if multiple processes attempted to access the same file at the same time and access to the file should have been allowed by an ACL on the file, access may have been denied instead.<br>• Fixes a problem where, if the ACL on a file wascorrupted,and the corrupted ACL was passed into the kernel, it caused a variety of problems.<br>• Fixes various problems in the ee driver for DE60x Ethernet adapters.<br>• Fixes an I/O hang condition on FibreChannel. |
| Patch 1109.00 OSF445-723 | **Patch:** Fixes problem where tape read/write operations fail<br>**State:** New. Supersedes patch OSF445-251 (758.00)<br>This patch corrects the following:<br>• Fixes a problem when the type of SCSI device dynamically changes, which can result in a kernel memory fault or memory corruption panic.<br>• Corrects a problem where interrupting an aseagent daemon with a signal can cause devices to become unaccessible.<br>• Fixes the problem where tape read/write operations fail with the following repetitive binary.errorlog message:<br>ctape_strategy: Device state flags indicate a Reserve is Pending<br>• Tapes reporting a SCSI version other than 2 would not work properly. |
| | |
| | |

# 3

# Summary of TruCluster Software Patches

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

**Table 3–1: Summary of TruCluster Patches**

| Patch IDs | Abstract |
|---|---|
| Patch 4.00<br>TCR160-004 | **Patch:** Fix for Kernel Memory Fault On DRD Client Nodes<br>**State:** Existing<br>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<br>TCR160-010 | **Patch:** Fix for Reliable Datagram API<br>**State:** Supersedes patch TCR160-001 (1.00)<br>This patch corrects the following:<br>• Reliable Datagram (RDG) messaging support.<br>• RDG: bug fix to the completion queue synchronization protocol. |
| Patch 8.00<br>TCR160-011 | **Patch:** doconfig may hang when running in TruCluster environment<br>**State:** Existing<br>This patch fixes two problems that could cause doconfig to appear to hang when running in a TruCluster environment. |
| Patch 33.00<br>TCR160-037 | **Patch:** Fix for drdadmin problems<br>**State:** Existing<br>This patch fixes various problems with drdadmin to be user friendly. |
| Patch 34.00<br>TCR160-038 | **Patch:** Fixes a limitation in ase_reconfig_bus<br>**State:** Existing<br>This patch fixes a limitation in ase_reconfig_bus. Now up to 99 buses can be reconfigured with this command. |
| Patch 36.00<br>TCR160-040 | **Patch:** Fix for asedirector hang<br>**State:** Existing<br>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. |

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

| | |
|---|---|
| Patch 61.00<br>TCR160-054B | **Patch:** Fixes problems with the clu_ivp script<br>**State:** Supersedes TCR160-009B (22.00), TCR160-021B (23.00), TCR160-022B (24.00), TCR160-031B (25.00), TCR160-036B (50.00), TCR160-047B (51.00)<br>This patch corrects the following:<br>• This is a performance improvement in the startup of start scripts. It will reduce the necessary system calls to start the scripts.<br>• Corrects a problem with member add in a large environment.<br>• Corrects a problem which causes asemgr to core dump when modifying a single DRD service to add more than 200 devices.<br>• Fixes a problem that caused aseagent or asehsm to core dump when starting NFS and Disk Services that contain several LSM volumes.<br>• Fixes a problem with extraneous compiler warnings about strdup() function calls from ASE.<br>• 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.<br>• This patch fixes the following problems with the clu_ivp script:<br>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 buses if none are listed in the configuration file. |
| Patch 65.00<br>TCR160-063 | **Patch:** Unable to remove LSM volumes from DRD service<br>**State:** Supersedes patch TCR160-003 (3.00)<br>This patch corrects the following:<br>• Fixes a problem where DRD permissions could be lost if a service is modified more than once.<br>• Fixes a problem that prevented the removal of LSM volumes from a DRD service. The problem occurs when there are multiple LSM disk groups in the service, and all of the volumes from one disk group were removed. |
| Patch 70.00<br>TCR160-056 | **Patch:** TruCluster Production Server hangs during boot<br>**State:** Supersedes patches TCR160-017 (11.00), TCR160-027 (19.00), TCR160-032 (26.00), TCR160-062 (68.00)<br>This patch corrects the following:<br>• Fixes a problem where both nodes in a cluster will panic at the same time with a simple_lock timeout panic.<br>panic (cpu 0): rm_update_single_lock_miss: time limit exceeded<br>• Fixes a problem that could cause an error to be returned when the cluster software should wait until a global lock is freed.<br>• 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<br>TCR160-067 | **Patch:** Error msg if system contained unsupported controllers<br>**State:** Existing<br>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<br>TCR160-061 | **Patch:** Access mode for a directory not set to default<br>**State:** Supersedes patches TCR160-045 (41.00), TCR160-048 (44.00), TCR160-049 (45.00)<br>This patch corrects the following:<br>• Fixes a problem that caused the setting of the "force unmount" option to be incorrectly displayed by the asemgr utility.<br>• Fixes a problem that caused shell errors if an invalid mount option was specified via the asemgr menu.<br>• 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.<br>• 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<br>TCR160-055 | **Patch:** Problem causes mountd to exit without error<br>**State:** Existing<br>This patch fixes a problem that could cause mountd to exit without error during boot. |
| Patch 80.00<br>TCR160-070 | **Patch:** Fixes problem with ASE_SNMPD_IGNORE_DISKS<br>**State:** New<br>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<br>TCR160-077 | **Patch:** Fixes a problem that causes asedirector to core dump<br>**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)<br>This patch corrects the following:<br>• Corrects a problem with NetWorker displaying garbage characters following service names. It occurs when the service name is 8 characters or greater.<br>• Fixes two problems in the asedirector:<br>– An ASE command timeout problem encountered by large ASE services.<br>– An incorrect decision made by the asedirector as a result of a failed inquire services command. |

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

| | |
|---|---|
| Patch 88.00 continued | • This is a performance improvement in the startup of start scripts. It will reduce the necessary system calls to start the scripts.<br>• 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.<br>• Fixes an ASE problem where, under certain circumstances, the service scripts could cause the ASE agent to loop during a start or stop service.<br>• Corrects a problem with member add in a large environment.<br>• Corrects a problem with a 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.<br>• 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.<br>• Corrects a problem which causes asemgr to core dump when modifying a single DRD service to add more than 200 devices.<br>• Fixes a problem that caused aseagent or asehsm to core dump when starting NFS and Disk Services that contain several LSM volumes.<br>• Fixes a problem where the asemgr will hang as it continuously create and kill multiple directors.<br>• Corrects a problem that causes the ASE director to core dump during initialization.<br>• 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.<br>• 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.<br>• 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.<br>• Fixes a problem that caused the asemgr to get a memory fault when adding multiple services in a row.<br>• Fixes a problem with extraneous compiler warnings about strdup() function calls from ASE. |

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

| | |
|---|---|
| Patch 88.00 continued | • 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.<br>• Fixes a problem that can cause the Cluster MIB daemon (cnxmibd) to core dump in Available Server environments.<br>• Fixes a problem which caused an error message to be logged for the cnxmibd even though no error had occurred.<br>• Fixes two issues with clusters:<br>– When a cluster is brought up with ASE off, other members report it as UP and RUNNING instead of UP and UNKNOWN.<br>– 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.<br>• Fixes a problem where timeout values of greater than 30 seconds in /etc/hsm.conf would cause ASE agent to fail at start up.<br>• Fixes a bug where the aseagent will occasionally core dump on a SCSI bus hang.<br>• Fixes a problem that caused the asemgr to report the wrong status for a service.<br>• This patch fixes the following problems with the clu_ivp script:<br>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 buses if none are listed in the configuration file.<br>• Fixes a problem that could cause the asedirector to core dump.<br>• Fixes a problem that caused the asemgr to report that a disk, or mount point, was in multiple services when modifying a service name.<br>• Fixes a problem with the ASE application from reporting an incorrect status while booting, after installation or while reinitializing the database. |
| Patch 90.00<br>TCR160-080 | **Patch:** Node crashes when holding an mc-api lock<br>**State:** Supersedes patches TCR160-029 (20.00), TCR160-050 (46.00), TCR160-064 (63.00)<br>This patch corrects the following:<br>• 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.<br>• Fixes a problem that can cause a panic in mcs_wait_cluster_event() when using the Memory Channel API.<br>• Fixes a problem with the Memory Channel API whereby a node crashes holding an mc-api lock. Under certain circumstances the lock will not be released after the node crashes.<br>• Fixes a problem in the Memory Channel API that can cause a system to hang. |
| Patch 92.00<br>TCR160-082 | **Patch:** Routing info for ASE service not properly updated<br>**State:** New<br>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<br>TCR160-072 | **Patch:** LSM disk information not updated in ASE database<br>**State:** Supersedes patches TCR160-030 (28.00), TCR160-039 (35.00)<br>This patch corrects the following:<br>• 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.<br>• Fixes a problem where LSM disk information was not properly updated in the ASE database when volumes were removed from a disk service.<br>• Fixes a problem with updating ASE services which involve deleting and adding AdvFS domains on LSM volumes. |
| Patch 97.00<br>TCR160-074 | **Patch:** Processes may get referenced several times<br>**State:** Supersedes patches TCR160-008 (6.00), TCR160-023 (15.00), TCR160-044 (40.00), TCR160-046 (42.00), TCR160-073A (95.00)<br>• Fixes a problem in which a cluster node can panic with the panic string "convert_lock: bad lock state".<br>• 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.<br>• Fixes a problem that can cause a TruCluster member to panic during shutdown.<br>• Fixes a bug where sometimes a certain shared sequence number will not be freed after use. It also fixes a problem where certain processes could get referenced several times.<br>• Fixes an Oracle process hang if a node fails after receiving a rsbinfo message.<br>• Fixes a DLM problem where two processes could take out the same lock. |
| Patch 99.00<br>TCR160-073B | **Patch:** clu_ivp script enhancements<br>**State:** Supersedes patch TCR160-054C (67.00)<br>This patch corrects the following:<br>• This patch fixes the following problems with the clu_ivp script:<br>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.<br>• Fixes an Oracle process hang if a node fails after receiving a rsbinfo message. |
| Patch 101.00<br>TCR160-081 | **Patch:** clu_ivp does not recognize Emulex adapter<br>**State:** Supersedes patch TCR160-041 (37.00)<br>This patch corrects the following:<br>• Fixes a problem where the Emulex Fibre Channel adapter was not recognized by clu_ivp.<br>• 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<br>TCR160-083 | **Patch:** Fix for boot failure on a cluster<br>**State:** Supersedes patches TCR160-034 (30.00), TCR160-068 (82.00)<br>This patch corrects the following:<br>• Fixes a problem which caused a boot failure on a cluster with a large number of shared SCSI buses.<br>• Fixes a problem in clustered systems. It reduces the occurrences of tmv2_notify_cbf error messages in the errlog.<br>• Fixes a possible system hang during shutdown due to a process having an active light weight wiring. |
| Patch 105.00<br>TCR160-084 | **Patch:** Corrects a problem in Memory Channel<br>**State:** New<br>This patch corrects a problem in the Memory Channel that can cause communication to stop and cause erroneous network partitions. |