DIGITAL UNIX

Patch Summary and Release Notes for DIGITAL UNIX V4.0C, Patch Kit-0007

April 1999

This manual describes the release notes and contents of Patch Kit-0007. It provides any special instructions for installing individual patches.

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

Compaq Computer Corporation
Houston, Texas

Contents

About This Manual

This manual contains information specific to Patch Kit-0007 for the DIGITAL UNIX Version 4.0C operating system and products. It provides a list of the patches contained in each kit and describes any information you need to know when installing specific patches.

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

Audience

This manual is for the person who installs and removes the patch kit and for anyone who manages patches after they are installed.

Organization

This manual is organized as follows:

Chapter 1 Contains the release notes for this patch kit.

Chapter 2 Summarizes the base operating system 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 DIGITAL UNIX and TruCluster documents:

- DIGITAL UNIX, ASE, and TCR *Patch Kit Installation Instructions*
- DIGITAL UNIX *Installation Guide*
- DIGITAL UNIX *System Administration*
- TruCluster Software Products *Software Installation*
- TruCluster Software Products *Administration*
- Any release-specific installation documentation

Reader's Comments

Compaq welcomes any comments and suggestions you have on this and other DIGITAL 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 DIGITAL UNIX that you are using.
- If known, the type of processor that is running the DIGITAL UNIX software.

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

1

Release Notes

This chapter provides information that you must be aware of when working with DIGITAL UNIX 4.0C Patch Kit-0007.

1.1 Required Storage Space

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

Base Operating System

- Temporary Storage Space

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

- Permanent Storage Space

  Up to ~45 MB of storage space in `/var/adm/patch/backup` may be required for archived original files if you choose to install and revert all patches. See the *Patch Kit Installation Instructions* for more information.

  Up to ~46 MB of storage space in `/var/adm/patch` may be required for original files if you choose to install and revert all patches. See *Patch Kit Installation Instructions* for more information.

  Up to ~769 KB of storage space is required in `/var/adm/patch/doc` for patch abstract and README documentation.

  A total of ~105 KB of storage space is needed in `/usr/sbin/dupatch` for the patch management utility.

1.2 New dupatch Features

The following sections describe new features of `dupatch`.

1.2.1 Dupatch-based Patch Kits for ASE and TCR Patches

Patches for ASE and TCR are now installed, removed, and managed through `dupatch`. The ASE and TCR patch kits have been converted to `dupatch`-based patch kits and distributed in the same patch distribution as the applicable operating system.

The multi-product support within `dupatch` is most visible when installing or removing patches. `dupatch` will display a list of the products which are on the system and in the patch kit, allowing the user to select one or more products before proceeding with patch selections.

You must load the new patch tools provided in this patch kit. See the *Patch Kit Installation Instructions* for more information.

Since all prior ASE and TCR patches have been installed manually, you must set the system patch baseline. See the *Patch Kit Installation Instructions* for detailed information.

1.2.2 New Cross-Product Patch Dependency Management

The dupatch utility now manages patch dependencies across the DIGITAL UNIX operating system, ASE, and TCR patch kits. An example of patch cross-product dependency handling for a system with both DIGITAL UNIX 4.0C and TCR 1.5 installed follows:

- If a DIGITAL UNIX 4.0C Patch 1.00 is chosen for installation and it depends upon TruCluster 1.5 Patch 17.00 which is not already installed or chosen for installation, the dupatch installation precheck will warn you of the dependency and block the installation of the DIGITAL UNIX 4.0C Patch 1.00.

  If the patch selections are reversed, dupatch will still warn you and block installation of the chosen patch.

1.2.3 Patch Special Instruction Handling by dupatch

The format and content of the per-patch special instructions has been revised to make it easier to use. The special instructions are now displayed when patches are removed. The per-patch special instructions are viewable through the dupatch documentation menu.

1.2.4 Patch Tracking and Documentation Viewing

The patch tracking and documentation viewing features within dupatch can now be used in multi-user mode by non-root users. See the *Patch Kit Installation Instructions* for more information.

From the dupatch patch tracking menu you can now list the patch kits from which patches installed on your system originated.

1.2.5 System Patch Baselining

The system patch baselining feature of dupatch has been improved. Phase 4 now reports all missing or unknown system files regardless of their applicability to the patch kit. This will help you identify the origin of manually changed system files. See the *Patch Kit Installation Instructions* for more information.

1.2.6 New Command Line Interface Switches

The dupatch command line mode contains the following new switches:

- The -product switch must be used when you specify the -install or -delete switches when the target system has more than one installed product that is on the kit (such as DIGITAL UNIX, ASE, and TCR). This switch allows you to specify the product name which the rest of the patch operations will affect. The -product switch must precede the -patch switch on the command line. See the *Patch Kit Installation Instructions* for more information.
- A -nolog switch has been added to enable you to turn off session logging.
- The -version switch is no longer used for delete. Using this switch will cause an error and the help information will be displayed on the screen.

Any error on the command line will cause the help information to be displayed on the screen.

If any mandatory switch is missing when using the command line interface, the command fails with the appropriate usage message. Once you select the command

line interface, dupatch will not go into interactive mode. Prompting is no longer mixed with the command line interface.

1.2.7 Compatibility Between Revisions of dupatch

The new dupatch will work with older revisions of dupatch-based patch kits.

The older revisions of dupatch, however, rev 15 and lower, do not know how to install, remove, or manage patches from the new style patch kits. Please ensure that you load the new patch installation tools when you receive this patch kit. See the *Patch Kit Installation Instructions* for more information.

1.3 Release Note for Nonreversible Install

An fgrep message may appear while installing all the patches as nonreversible, or while update installing a patched system to a later release; for example, V4.0D.

```
fgrep: input too long
```

You may ignore this message.

1.4 Release Note for Patch 673.00

The following represents an update to the cc(1) reference page:

A new switch, -input_to_ld, has been added to the cc compiler.

This new switch allows the passing of the "-input filename" switch to ld via cc, without changing the file's relative position in the ld command line.

Note that using the -Wl switch to do this (-Wl, -input, filename) impacts the order in which files are presented to the linker and can result in an invalid executable being created. This is due to the cc compiler's convention of placing all arguments passed via -Wl on the command line first, followed by any switches or object files entered by the user on the cc command line that are meant for ld. This convention results in the .o files specified with -Wl, -input, filename to be included before all other .o files on the command line, and before /usr/lib/cmplrs/cc/crt0.o, which is the transfer point for all executables. The linker lays out the code in the order in which it sees the input .o files, so their order on the ld command line is important.

1.5 Release Note for Patch 693.00

The following is an update to the mount (8) reference page in the AdvFS Options section of the mount -o Flag Options:

atimes

Flushes to disk the file access time changes for reads of regular files.
This is the default XPG4 behavior.

noatimes

Marks file access time changes for reads of regular files in memory, but does not flush them to disk until other file modifications occur. This behavior does not comply with industry standards and is used to reduce disk writes for applications with no dependencies on file access times.

read(2):

[DIGITAL] If the file is a regular file and belongs to an AdvFS fileset mounted with the AdvFS option noatimes, the read, readv, or pread function marks the st_atime field of the file for update. If the file otherwise remains unchanged, the new st_atime value is not flushed to disk. See mount(8) for more information on the noatimes mount option.

The following is an update to the *System Configuration and Tuning Guide,* Appendix B, Section 1, "AdvFS Subsystem Attributes":

AdvfsPreallocAccess

AdvFS will allocate this number of access structures to the AdvFS access structure freelist at startup. The minimum value is 128, the maximum value is 65536. The actual value allocated at startup will be adjusted to honor the AdvfsAccessMaxPercent configurable.

Default value: 128

On larger systems, a larger value than the default value of 128 may improve performance by slowing the rate of access structure recycling, allowing cached file metadata to stay in main storage.

1.6 Release Note for Patch 394.00

Before the line discipline streams module (`ldtty`) closes, it sleeps for 30 seconds, waiting for the write queue to drain. In this situation, the sleep time needs to be longer. There is a kernel global variable, `ldtty_drain_tmo`, that specifies this time. This variable can now be patched using `dbx`.

```
# dbx -k /vmunix

(dbx) print ldtty_drain_tmo
30
(dbx) patch ldtty_drain_tmo=60
60
(dbx) quit
#
```

Some experimentation may be necessary to find the correct value for a specific customer environment.

1.7 Release Notes for Patch 599.00

The following table lists the tape compatibility for the TZ85, TZ86, TZ87, TZ88, and TZ89 tape drives.

Table 1–1: Media Type for TZn Tape Drives

Media Type	Drive Type
CompacTapeI	TZ30, TK50
CompacTapeII	TZ30, TK50, TK70, TZ85, TZ86
CompacTapeIII	TZ85, TZ86, TZ87, TZ88, TZ89
CompacTapeIIIXT	TZ88, TZ89
CompacTapeIV	TZ88, TZ89

Table 1–2 provides information about TZ85, TZ86, TZ87, TZ88, and TZ89 tape drives. Note that in the capacity column, a number followed by an asterisk (*) assumes a 2:1 compression ratio. The actual compression ratio may vary depending on the type of data being compressed.

Table 1–2: Supported Formats for TZn Tape Drives

Format	Device Special	Density Code	Compression	Capacity	Cartridge	I/O Supported
TZ85	rmt?a	1ah	N/A	2.6 GB	CompacTape III	Read-only
TZ85	rmt?l	1ah	N/A	2.6 GB	CompacTape III	Read-only
TZ86	rmt?a	1ah	N/A	10.0 GB	CompacTape III	Read-only
TZ86	rmt?l	1ah	N/A	10.0 GB	CompacTape III	Read-only
TZ87	rmt?a	1ah	Off	10.0 GB	CompacTape III	Read-only
TZ87	rmt?l	1ah	On	20.0 GB*	CompacTape III	Read-only
TZ87	rmt?m	00h	Off	10.0 GB	CompacTape III	Read/write
TZ87	rmt?h	00h	On	20.0 GB*	CompacTape III	Read/write
TZ88	rmt?a	1ah	Off	15.0 GB	CompacTapeIIIXT	Read-only
TZ88	rmt?l	1ah	Off	30.0 GB*	CompacTapeIIIXT	Read-only
TZ88	rmt?m	00h	Off	15.0 GB	CompacTapeIIIXT	Read/write
TZ88	rmt?h	00h	On	30.0 GB*	CompacTapeIIIXT	Read/write
TZ88	rmt?a	1ah	Off	20.0 GB	CompacTape IV	Read/write
TZ88	rmt?l	1ah	On	40.0 GB*	CompacTape IV	Read/write
TZ89	rmt?a	1ah	Off	15.0 GB	CompacTapeIIIXT	Read-only
TZ89	rmt?l	1ah	Off	30.0 GB*	CompacTapeIIIXT	Read-only
TZ89	rmt?m	00h	Off	15.0 GB	CompacTapeIIIXT	Read/write
TZ89	rmt?h	00h	On	30.0 GB*	CompacTapeIIIXT	Read/write
TZ89	rmt?m	00h	Off	35.0 GB	CompacTape IV	Read/write
TZ89	rmt?h	00h	On	70.0 GB*	CompacTape IV	Read/write

Table 1–3 lists the tape compatibility for the TLZ04, TLZ06, TLZ07, TLZ09, and TLZ10 tape drives.

Table 1–3: Tape Compatibility for TLZn Tape Drives

Media Type	Drive Type
DDS-1 (60m)	TLZ04, TLZ06, TLZ07, TLZ09, TLZ10
DDS-1 (90m)	TLZ06, TLZ07, TLZ09, TLZ10
DDS-2 (120m)	TLZ07, TLZ09, TLZ10
DDS-3 (125m)	TLZ10

Table 1–4 provides information about the TLZ–family of tape drives. The TLZ10 tape drives support variable block size. Note that in the capacity column, a number followed by an asterisk (*) assumes a 2:1 compression ratio. The actual compression ratio may vary depending on the type of data being compressed.

Table 1–4: Supported Formats for TLZ10 Tape Drives

Format	Device Special	Density Code	Compression	Capacity	Cartridge	I/O Supported
TLZ04	rmt?a	00h	N/A	1.3 GB	DDS-1 (60m)	Read/Write
TLZ04	rmt?l	00h	N/A	1.3 GB	DDS-1 60m)	Read/Write
TLZ04	rmt?m	00h	N/A	1.3 GB	DDS-1 (60m)	Read/Write

Table 1–4: Supported Formats for TLZ10 Tape Drives (cont.)

TLZ04	rmt?h	00h	N/A	1.3 GB	DDS-1 (60m)	Read/Write
TLZ06	rmt?a	00h	Off	1.3 GB	DDS-1 (60m)	Read/Write
TLZ06	rmt?l	00h	Off	1.3 GB	DDS-1 (60m)	Read/Write
TLZ06	rmt?m	00h	On	2.6 GB *	DDS-1 (60m)	Read/Write
TLZ06	rmt?h	00h	On	2.6 GB *	DDS-1 (60m)	Read/Write
TLZ06	rmt?a	00h	Off	2.0 GB	DDS-1 (90m)	Read/Write
TLZ06	rmt?l	00h	Off	2.0 GB	DDS-1 (90m)	Read/Write
TLZ06	rmt?m	00h	On	4.0 GB *	DDS-1 (90m)	Read/Write
TLZ06	rmt?h	00h	On	4.0 GB *	DDS-1 (90m)	Read/Write
TLZ07	rmt?a	00h	Off	4.0 GB	DDS-2	Read/Write
TLZ07	rmt?l	00h	Off	4.0 GB	DDS-2	Read/Write
TLZ07	rmt?m	00h	On	8.0 GB *	DDS-2	Read/Write
TLZ07	rmt?h	00h	On	8.0 GB *	DDS-2	Read/Write
TLZ09	rmt?a	00h	Off	4.0 GB	DDS-2	Read/Write
TLZ09	rmt?l	00h	Off	4.0 GB	DDS-2	Read/Write
TLZ09	rmt?m	00h	On	8.0 GB *	DDS-2	Read/Write
TLZ09	rmt?h	00h	On	8.0 GB *	DDS-2	Read/Write
TLZ10	rmt?a	00h	Off	12.0 GB	DDS-3	Read/Write
TLZ10	rmt?l	00h	Off	12.0 GB	DDS-3	Read/Write
TLZ10	rmt?m	00h	On	24.0 GB *	DDS-3	Read/Write
TLZ10	rmt?h	00h	On	24.0 GB *	DDS-3	Read/Write

Table 1–5: Supported Formats for TZS20 Tape Drives

Format	Device Special	Density Code	Compression	Capacity	Cartridge	I/O Supported
TZS20	rmt?a	00h	Off	25.0 GB	AIT	Read/Write
TZS20	rmt?l	00h	Off	25.0 GB	AIT	Read/Write
TZS20	rmt?m	00h	On	50.0 GB *	AIT	Read/Write
TZS20	rmt?h	00h	On	50.0 GB *	AIT	Read/Write

1.8 Release Note for Patch 393.00

The binlogd daemon sends messages to the filterlog utility. The filterlog utility keeps track of correctable CPU errors and reports them when a threshold has been reached.

The syntax is as follows:

```
filterlog [-d crdlog] [-s crdlength #] [-s crdcount #] [-s crdincrement
#] [-l]

FLAGS
  -d crdlog         - Dumps the CRD log.
  -d crdlifetime    - Dumps the CRD lifetime log.
  -l                - Logs entry read in from stdin. Used by binlogd.
  -s crdlength #    - Set the CRD interval time in minutes (24 hour
default).
  -s crdcount #     - Set the CRD interval count (50 default).
  -s crdincrement # - Set the CRD interval increment (100 default).
```

1.9 Release Note for Patch 569.00

The following sections contain reference page updates.

1.9.1 Reference Page Update for cron(8)

1. Add the following to the DESCRIPTION section:

   When the `cron` daemon is started with the `-d` option, a trace of all jobs executed by `cron` is output to file `/var/adm/cron/log`.

2. Add the following to the FILES section:

   ```
   /var/adm/cron/cron.deny
      List of denied users
   /var/adm/cron/log
      History information for cron
   /var/adm/cron/queuedefs
      Queue description file for at, batch, and cron
   ```

3. Add `queuedefs(4)` to the Files: section of RELATED INFORMATION.

1.9.2 New Reference Page for queuedefs(4):

queuedefs(4) queuedefs(4)

NAME

queuedefs - Queue description file for at, batch, and cron commands

DESCRIPTION

The queuedefs file describes the characteristics of the queues managed by cron or specifies other characteristics for cron. Each non-comment line in this file describes either one queue or a cron characteristic. Each uncommented line should be in one of the following formats.

```
q.[njobj][nicen][nwaitw]
max_jobs=mjobs
log=lcode
```

The fields in these line are as follows:

q The name of the queue. Defined queues are as follows:

a The default queue for jobs started by at

b The default queue for jobs started by batch

c The default queue for jobs run from a crontab file

Queues d to z are also available for local use.

njob The maximum number of jobs that can be run simultaneously in the queue; if more than njob jobs are ready to run, only the first njob jobs will be run. The others will be initiated as currently running jobs terminate.

nice The nice(1) value to give to all jobs in the queue that are not run with a user ID of superuser.

nwait The number of seconds to wait before rescheduling a job that was deferred because more than njob jobs were running in that queue, or because the system-wide limit of jobs executing (max_jobs) has been reached.

mjobs The maximum number of active jobs from all queues that may run at any one time. The default is 25 jobs.

lcode Logging level of messages sent to a log file. The default is 4.
Defined levels are as follows:

level-code level

0 None

1 Low

2 Medium

3 High

4 Full

Lines beginning with # are comments, and are ignored.

EXAMPLES

The following file specifies that the b queue, for batch jobs, can have up to 50 jobs running simultaneously; that those jobs will be run with a nice value of 20. If a job cannot be run because too many other jobs are running, cron will wait 60 seconds before trying again to run it. All other queues can have up to 100 jobs running simultaneously; they will be run with a nice value of 2, and if a job cannot be run because too many other jobs are running, cron will wait 60 seconds before trying again to run it.

```
b.50j20n60w
```

The following file specifies that a total of 25 active jobs will be allowed by cron over all the queues at any one time, and cron will log all messages to the log file. The last two lines are comments that are ignored.

```
max_jobs=25
log=4
# This is a comment
# And so is this
```

FILES

/var/adm/cron
Main cron directory

/var/adm/cron/queuedefs
The default location for the queue description file.

RELATED INFORMATION

Commands: at(1), cron(8), crontab(1), nice(1)

1.9.3 Reference Page Update for crontab(1):

On days when the daylight saving time (DST) changes, cron schedules commands differently from normal.

The 2 rules described below specify cron's scheduling policy for days when the DST changes. First some terms will be defined.

An AMBIGUOUS time refers to a clock time that occurs twice in the same day because of a DST change (usually on a day during Fall).

A NONEXISTENT time refers to a clock time that does not occur because of a DST change (usually on a day during Spring).

DSTSHIFT refers to the offset that is applied to standard time to result in daylight savings time. This is normally one hour, but can be any amount of time up to 23 hours and 59 minutes.

The TRANSITION period starts at the first second after the DST shift occurs, and ends just before DSTSHIFT time later.

An HOURLY command has a * in the hour field of the crontab entry.

RULE 1: (AMBIGUOUS times)

A non-hourly command is run only once at the first occurrence of an ambiguous clock time.

- A non-hourly command scheduled for 01:15 and 01:17 will be run at 01:15 and 01:17 EDT on 10/25/98 and will not be run at 01:15 or 01:17 EST.

An hourly command is run at all occurrences of an ambiguous time.

- An hourly command scheduled for *:15 and *:17 will be run at 01:15 and 01:17 EDT on 10/25/98 and also at 01:15 and 01:17 EST.

RULE 2: (NONEXISTENT times)

A command is run DSTSHIFT time after a nonexistent clock time.

If the command is already scheduled to run at the newly shifted time, then the command is run only once at that clock time.

- A non-hourly command scheduled for 02:15 and 03:15 will be run once at 03:15 EDT on 4/5/98.

- A non-hourly command scheduled for 02:15 and 02:17 will be run once at 03:15 and once at 03:17 EDT on 4/5/98.

- An hourly command scheduled for *:15 and *:17 will be run once at 03:15 and once at 03:17 EDT on 4/5/98.

Note:
Cron's behavior during the transition period is undefined if the DST shift crosses a day boundary, for example when the DST shift is 23:29:29->00:30:00 and the transition period is 00:30:00->01:29:59.

Here are sample DST change values (for Eastern US time EST/EDT). During the transition period, clock time may be either nonexistent (02:00-02:59 EST in Spring) or ambiguous (01:00-01:59 EDT or EST in Fall).

Spring (April 5, 1998):
DST shift: 01:59:59 EST –> 03:00:00 EDT
transition period: 03:00:00 EDT –> 03:59:59 EDT
DSTSHIFT: 1 hour forwards

Fall (Oct 25, 1998):
DST shift: 01:59:59 EDT –> 01:00:00 EST
transition period: 01:00:00 EST –> 01:59:59 EST
DSTSHIFT: 1 hour backwards

1.10 Release Note for Patch 542.00

The updated reference page sections for `lpr(1)` follow:

The printer log, lpr.log now reports the creation of files preceded by a dot (.) in the spooling directories. Do not amend or delete these files as the printer subsystem manages their creation and

cleanup.

For initial use, DIGITAL recommends that you set the logging level to lpr.info. If you have a problem that is escalated to technical support, the support organization will request lpr.log at the lpr.debug level. This is because the DEBUG messages provide a detailed trace that can only be interpreted by reference to the source code and lpr.log will simply grow more quickly if DEBUG messages are logged. The lpr.info level provides a shorter report of an event, including any network retry messages and unusual occurences (which are not always errors).

All changes to the status file of a queue, including reports of any files printed, are reported at the DEBUG level rather than the INFO level. This reduces the rate of growth of the file and allows you to monitor and react to important events more quickly. The WARNING level logs events that may need to be attended to, while the ERROR level logs hard (often fatal) errors.

To modify the logging level, edit your /etc/syslog.conf file and change the lpr line to the required level, such as lpr.info as follows:

```
lpr.info      /var/adm/syslog.dated
```

Use the ps command to find the PID for the syslog daemon, and the following command to re-start syslogd:

```
# kill -HUP
```

A new set of log files will be created in /var/adm/syslog.

2

Summary of Base Operating System Patches

This chapter summarizes the base operating system patches included in Patch Kit-0007.

Table 2–2 provides a summary of patches in.

Table 2–1: Updated Base Operating System Summary

Patch IDs	Change Summary
Patches 499.00, 707.00, 657.00, 693.00, 689.00, 509.00, 701.00, 696.00, 699.00, 541.00, 640.00, 627.00, 586.00, 676.00, 597.00, 673.00, 690.00, 500.00, 505.00, 510.00, 584.00, 563.00, 527.00, 539.00, 598.00, 622.00, 570.00, 576.00, 585.00, 594.00, 604.00, 621.00, 706.00, 644.00, 645.00, 647.00, 649.00, 667.00, 610.00, 501.00, 658.00, 650.00, 697.00, 703.00	New
Patches 125.00, 351.00, 353.00	Superseded by Patch 504.00
Patch 126.00	Superseded by Patch 502.00
Patch 128.00	Superseded by Patch 503.00
Patches 140.00, 201.00, 275.00	Superseded by Patch 698.00
Patches 201.00, 275.00	Superseded by Patch 655.00
Patches 30.00, 66.00, 147.00, 233.00, 254.00, 430.00	Superseded by Patch 634.00
Patches 43.00, 111.00, 111.01, 171.00	Superseded by Patch 599.00
Patches 44.00, 304.00	Superseded by Patch 700.00
Patches 221.01, 219.00, 91.00, 298.00, 416.00	Superseded by Patch 695.00
Patches 47.00, 33.00	Superseded by Patch 600.00
Patches 65.00, 69.00, 306.00, 410.00, 433.00	Superseded by Patch 532.00
Patches 82.00, 96.00, 173.00, 70.00, 308.00, 310.00, 490.00	Superseded by Patch 694.00
Patches 78.00, 321.00	Superseded by Patch 614.00
Patch 81.00	Superseded by Patch 651.00
Patches 84.00, 258.00, 450.00	Superseded by Patch 523.00
Patch 83.00	Superseded by Patch 552.00
Patch 94.00	Superseded by Patch 608.00
Patches 101.00, 289.00, 297.00, 368.00	Superseded by Patch 561.00
Patches 105.00, 105.01, 105.02, 437.00	Superseded by Patch 580.00
Patch 107.01	Superseded by Patch 623.00
Patches 107.00, 491.00	Superseded by Patch 704.00
Patch 119.00	Superseded by Patch 562.00
Patch 152.00	Superseded by Patch 555.00

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

Patches 154.00, 426.00	Superseded by Patch 593.00
Patches 145.00, 264.00, 486.00	Superseded by Patch 654.00
Patches 208.00, 367.00, 390.00	Superseded by Patch 681.00
Patch 158.00	Superseded by Patch 624.00
Patches 178.00, 236.00, 432.00	Superseded by Patch 518.00
Patch 184.00	Superseded by Patch 542.00
Patches 211.00, 358.00, 392.00	Superseded by Patch 637.00
Patch 270.00	Superseded by Patch 684.00
Patch 307.00	Superseded by Patch 545.00
Patches 301.00, 465.00	Superseded by Patch 569.00
Patch 318.00	Superseded by Patch 596.00
Patch 388.00	Superseded by Patch 661.00
Patch 476.00	Superseded by Patch 635.00
Patch 86.00	Superseded by Patch 568.00

Table 2–2: Summary of Base Operating System Patches

Patch IDs	Abstract
Patch 3.00 OSF415-410035	**Patch:** PCXAL, LK411, And Similar Keyboards **State:** Existing On systems with PCXAL, LK411, and similar keyboards, sometimes the keyboard stops working.
Patch 4.00 OSF415-410038	**Patch:** Change Cursor Reporting In The Workstation Driver **State:** Existing Issuing a SET_DEVICE_MODE ioctl to the workstation driver to change cursor reporting to relative mode fails.
Patch 14.00 OSF415-410053	**Patch:** Kernel Debugger Corrections **State:** Supersedes patch OSF415-410046 (9.00) This patch corrects the following: • Fixes a problem with the ikdebug debugger that causes a system to panic with the following message: panic: simple_lock: time limit exceeded • Fixes a problem in which an AlphaStation 600, as well as other systems, may crash when user mode debuggers are in use (for example, dbx or ladebug). • Reduces the kdebug memory usage. • Fixes user mode breakpoints/single stepping. • Fixes kdebug MP problems.
Patch 25.00 OSF415DX-410003	**Patch:** Environmental Monitoring Daemon Correction **State:** Existing This patch fixes the problem of the Environmental Monitoring daemon (envmond) failing to start sometimes when the system boots up.

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

Patch 41.00 OSF415-405063	**Patch:** libaio Correction **State:** Existing This patch fixes a problem that can occur with programs linked with libaio. These programs could dump core with a SIGSEGV signal or corrupt memory when calling the close() function with a bad file descriptor value.
Patch 42.00 OSF415X11-405005	**Patch:** ATI Mach64 Graphics Card Monitor Handling **State:** Existing On systems with an ATI Mach64 graphics card, sometimes the monitor will lose synchronization or become stuck in power-save mode.
Patch 56.00 OSF415-400126	**Patch:** Kernel Memory Fault Correction **State:** Existing This patch fixes a "kernel memory fault" in the dqget() routine.
Patch 77.00 OSF415-400166	**Patch:** Full Duplex Mode Setting on DEFPA Correction **State:** Existing This patch fixes a problem in which setting full duplex mode on DEFPA using "/usr/sbin/fddi_config -i fta0 -x1" will not enable full duplex mode.
Patch 79.00 OSF415-400168	**Patch:** netstat Command Output Correction **State:** Existing This patch fixes a problem in which "netstat -I fta0 -s" reports 6 bytes of the 8 byte "Station UID" and "Station ID".
Patch 87.00 OSF415-400179	**Patch:** CD/DSR Not Dropping Right Away After Dial-out **State:** Existing This patch corrects the following problem with uugetty — CD/DSR not dropping right away after dial-out.
Patch 88,00 OSF415-400183	**Patch:** rwhod Correction **State:** Existing This patch fixes a problem in which rwhod daemon can cause a core dump with a segmentation fault.
Patch 92.00 OSF415-400191	**Patch:** NTP Correction **State:** Existing This patch fixes a problem where the NTP deamon (xntpd) does not work using a Spectracom radio clock as a reference.
Patch 114.00 OSF415-400223	**Patch:** talkd Correction, Security (SSRT0446U) **State:** Existing A potential security vulnerability has been discovered in talkd, where under certain circumstances, system integrity may be compromised. DIGITAL has corrected this potential vulnerability.
Patch 127.01 OSF415CDE-400006-1	**Patch:** Nodename Length Correction **State:** Existing This patch fixes a problem in which users logging into a system that has a nodename longer than 32 characters cause ttsession to core dump. This only happens when using CDE desktop.

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

Patch 130.00 OSF415CDE-400009	**Patch:** dtksh Command Correction **State:** Existing Fixes two problems that occur when using the dtksh command: • dtksh can lose output lines when a pipe or I/O indirection is used. • The following error message may be displayed after using a pipe in dtksh: dtksh: hist_flush: EOF seek failed errno=9
Patch 133.00 OSF415DX-400007	**Patch:** DECwindows Session Manager Correction **State:** Existing This patch fixes the following problems in the DECwindows Session Manager (dxsession) application. Ungraceful exit can be made through the window manager's 'Close' button, whose behavior is inconsistent with that of dxsession's 'End Session' button.
Patch 141.00 OSF415X11-400011	**Patch:** S3 Trio64 Graphics Card Can Lose Time **State:** Existing Systems with an S3 Trio64 graphics card can lose time (on the order of a few minutes a day).
Patch 168.01 OSF415-400189C-1	**Patch:** uucp Command Correction, Security (SSRT0296U) **State:** Supersedes patch OSF415-400189 (91.00) This patch corrects the following: • A potential security vulnerability has been discovered in BIND (Domain Name Service), where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability. • Allows the uusend voliod commands to work correctly when the customer builds a hashed passwd database using a non-default page file block size.
Patch 169.00 OSF415-018	**Patch:** comm Command Correction **State:** Existing This patch fixes a problem in the comm command where it will split long line(s) in a file by inserting a line(s) in a file by inserting a <carriage return> that exceeds 255 characters. In some cases, characters will be truncated.
Patch 172.00 OSF415-400263	**Patch:** Patch: ar Command Correction **State:** Existing This patch fixes the following problems with the ar command: • When creating or modifying an archive, the ar command may leave a large file in /tmp or in the current directory (when the -l option is used). • If Patch 46.00 was previously installed (OSF400-046), the ar command cannot find object modules specified for deletion or extraction if the file name is longer than 13 characters. An error message similar to the following is displayed: ar: Error: button_previous.gif not found

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

Patch 175.00 OSF415-400268	**Patch:** Problem, System Time Using MICRO_TIME Kernel Config **State:** Existing This patch fixes several problems with system time when the MICRO_TIME kernel configuration option is used. • It resolves a one second delay in updating secondary processors after changing the system time. • BOOTTIME is now written properly to utmp from a secondary processor during boot. • Processors are immediately updated when brought on-line during boot or via the psradm utility.
Patch 176.00 OSF415-400269	**Patch:** yppasswd Command Correction **State:** Existing This patch fixes a problem in which yppasswd users get the error "password mismatch, password unchanged" creating passwords longer than 8 characters.
Patch 186.00 OSF415-400295	**Patch:** HX (PMAGB-BA) Graphic Mouse Cursor Correction **State:** Existing This patch fixes a problem with the mouse cursor when the system contains the HX (PMAGB-BA) graphics option. The cursor offset is incorrect on the Y Axis by 2 pixels.
Patch 193.00 OSF415-410078	**Patch:** inetd Enhancement **State:** Existing Enhanced /usr/sbin/inetd.
Patch 194.00 OSF415-410079	**Patch:** vipw Issues Warnings Enhancement **State:** Existing /usr/sbin/vipw now issues warning when used to edit a large password file.
Patch 196.00 OSF415-410081	**Patch:** removeuser Calls userdel Deletes Users Account **State:** Existing The script /usr/sbin/removeuser now calls /usr/sbin/userdel to do the actual work of deleting a user's account.
Patch 199.00 OSF415-400305	**Patch:** diff Command Correction **State:** Existing This patch fixes a problem related to misinterpretation of multibyte characters by the diff command. The problem also affects the delta command of SCCS. The symptom of the problem in the diff command is that it sometimes treats a text file containing multibyte characters as a binary file. The symptom of the problem in the delta command is that it sometimes fails to check in a program source file containing multibyte characters.
Patch 210.00 OSF415-410091	**Patch:** PowerStorm 3D30 PBXGB-AA 4D20 PBXGB-CA Correction **State:** Existing AlphaStation 255 systems with a PowerStorm 3D30 (PBXGB-AA) or PowerStorm 4D20 (PBXGB-CA) graphics card may hang, halt, or crash.
Patch 212.00 OSF415-405087	**Patch:** PCI Device Using Dense Space I/O Correction **State:** Existing This patch fixes a problem in which an AlphaServer 4100 with a PCI device that uses dense space I/O handles will panic with the following error message: panic: Machine Check 670

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

Patch 218.00 OSF415-410093	**Patch:** Patch: shutdown -r Command Correction **State:** Existing Fixes a problem that occurs on an AlphaServer 2100A system. When the system is shut down using the "shutdown -r" command, the system will not reboot.
Patch 222.00 OSF415-400331B	**Patch:** uusend And uustat Command Correction **State:** Supersedes patch OSF415-400331 (221.00) Allows the uusend, uustat, uucpd, and uudecode commands to work correctly when the customer builds a hashed passwd database using a non-default page file block size.
Patch 223.00 OSF415-410100	**Patch:** adduser Calls useradd To Create New User Account **State:** Existing The shell script /usr/sbin/adduser now calls /usr/sbin/useradd to do the actual work of creating the new user account. Duplicate UIDs are now permitted.
Patch 225.00 OSF415-400331C	**Patch:** mkpasswd -s Command Correction **State:** Supersedes patch OSF415-400331 (221.00) Allows customers to create hashed passwd databases from large passwd files by using a new option (-s) to the mkpasswd command. The -s option increases the block size of the database page file.
Patch 226.00 OSF415-400331D	**Patch:** voliod Command Correction **State:** Supersedes patch OSF415-400331 (221.00) This patch allows the uusend voliod commands to work correctly when the customer builds a hashed passwd database using a non-default page file block size.
Patch 230.00 OSF415-400282	**Patch:** quotas For Filesystems Causes rpc.rquotad To Hang **State:** Supersedes patch OSF415-400214 (106.00) This patch corrects the following: • Fixes a problem in which the rpc.rquotad daemon hangs when using quotas for NFS filesystems in a TruCluster or Available Server (ASE) V1.4 environment. • Fixes the following problems with the rpc.rquotad: – When the NFS server is a member of an ASE or TruCluster environment, the rpc.rquotad daemon may exit abnormally. The abnormal exit causes the quota command on NFS clients to not report quotas for NFS mounted file systems. – When the quota command is repeatedly run from a remote system, the virtual size of the rpc.rquotad daemon on the local system will grow due to a memory leak.
Patch 234.00 OSF415-400325	**Patch:** atom Command Corrections **State:** Existing This patch corrects the following: • The atom command terminates with SIGSEVG signal if the threaded program being instrumented has a stripped shared library. • The "atom -all -env threads" command produces an instrumented version of a threaded (eg DCE) application that will not execute correctly, with either "-tool third" or "-tool hiprof" tool options.

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

Patch 238.00 OSF415-400337	**Patch:** doconfig Utility Correction **State:** Existing This patch fixes a problem that causes the 'doconfig' program to hang when invoked by the uuxqt program.
Patch 239.00 OSF415-400340	**Patch:** date Command Correction **State:** Existing This patch fixes the problem in which 'date' command is unable to set the date to January 1, 1970 00:00:00 GMT or February 29, 2000.
Patch 248.00 OSF415-400358	**Patch:** awk Utility Correction **State:** Supersedes patch OSF415-400318 (205.00) This patch corrects the following: • Fixes problem in which 'awk' consume memory until the machine swaps itself and core dumps with following error: write failed, file system is full Memory fault - core dumped • Fixes a problem in which the awk -FS command does not display the correct output.
Patch 249.00 OSF415-400359	**Patch:** auditmask Utility Correction **State:** Existing This patch fixes a problem that affects systems running the audit subsystem. When reading directives from a file, the auditmask utility does not correctly handle lines formatted as follows: event fail
Patch 250.01 OSF415-400362-1	**Patch:** libm Correction **State:** Supersedes patches OSF415-400083 (46.00), OSF415-400293 (185.00) This patch corrects the following: • Fixes the problem of the math library functions not returning the correct NaN value as defined in the *Alpha AXP Architecture Reference Manual* (Second Edition). • Fixes a problem with fastmath functions F_Exp() and F_Pow() that would cause floating exception core dumps.
Patch 251.00 OSF415-400364	**Patch:** System Run Level Correction **State:** Existing This patch fixes two system run level problems: • On a system running LSM, whenever there is a run level change, the lsmbstartup script runs. This causes root to be mounted read/write in single-user mode. • The bcheckrc command script continues to run even if there is an invalid root entry. This leaves the system in an unusable state in single-user mode.
Patch 252.01 OSF415-400365-1	**Patch:** btree File Format Correction, Static Library **State:** Existing Fixes a probem that affects systems using databases with the btree file format. Only applications using btree in libdb.a or libdb.so are affected and may return incorrect data or crash.
Patch 256.00 OSF415-400370	**Patch:** Correction To volunroot, volrootmir, vol-reconfig **State:** Existing Fixes several LSM problems related to the volunroot, volrootmir, and vol-reconfig scripts.

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

Patch 259.01 OSF415-400371-1	**Patch:** uprofile and kprofile Command Corrections **State:** Existing This patch corrects the following: • The uprofile and kprofile commands report incorrect statistics on an SMP system or when trying to measure EV5 events other than cycles. • The pfm driver ioctl PCNT5GETCNT returns incorrect data. • An unstoppable stream of pfm interrupts is produced if an EV5 machine is rebooted with the pfm driver active. • The pfm(8), uprofile(1), and kprofile(1) manpages do not describe the EV5 statistics supported by the software. All users of the pfm driver and uprofile or kprofile commands should install this patch.
Patch 260.00 OSF415CDE-400011	**Patch:** dtmail Correction **State:** Existing This patch lets dtmail correctly display Japanese and Korean mail messages that do not have a Content-Type header.
Patch 261.00 OSF415DX-400012	**Patch:** Security Patch, (SSRT0514U) **State:** Existing A potential security vulnerability has been discovered, where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability.
Patch 262.00 OSF415X11-400018	**Patch:** X server Correction **State:** Existing The X server can loop or run out of sockets when dealing with a font server.
Patch 263.00 OSF415X11-400019	**Patch:** DECwindows Motif toolkit **State:** Existing Fixes the following problem in the Bookreader library, which is part of the DECwindows Motif toolkit. When called from an application, Bookreader changes the caller's effective UID to the real UID, but then never restores it to the original effective UID, before returning control to the calling program. If an application like dxchpwd is run from a non-root account, it fails with a privilege violation.
Patch 265.00 OSF415-405078	**Patch:** DLI Applications Correction **State:** Existing This patch fixes a problem that prevented DLI applications from working over-funneled drivers.

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

Patch 269.00 OSF415-410097	**Patch:** btextract Utility Correction **State:** Supersedes patches OSF415-410047 (10.00), OSF415-410056 (15.00) This patch corrects the following: • Fixes an automatic reboot problem when the system is booted from tape using the custom_install.sh file in a mini-root environment. • Fixes problems encountered when restoring file systems from a tape device using the btextract utility. • This patch fixes several problems for Bootable Tape: – While restoring the filesystem from the tape, the filesystem size selected was not sufficient to restore the contents from the tape. – The information message for restoring AdvFS additional volumes was not informative. – The SWAP SELECTION code for attended restore was failing while restoring customized disks with not default disklabels. – Extra mkdir statement was printing on the terminal. – The error status from "mt" command was not being checked. – Relative path for -s filename was not being accepted by btcreate. – The estimated size of the root filesystem should be corrected. – The file systems are not mounted automatically by btcreate. – The reboot command does not reboot the system while booted from the tape.
Patch 271.00 OSF415-410106	**Patch:** Corrects X.25 Crash On AlphaServer 1000 **State:** Existing Fixes a problem in which the io_zero() system call returns an incorrect value on an AlphaServer 1000.
Patch 273.00 OSF415-410108	**Patch:** Kernel Memory Fault Correction **State:** Existing An AlphaServer 4100 may panic with a kernel memory fault during boot under the following conditions: • The system has more than 32 MB of memory. • The console variable MEMORY_TEST is set to "partial"
Patch 292.00 OSF415-400383	**Patch:** Correction To llogin Command **State:** Existing Corrects a problem when exiting an llogin session. If the user does not enter a carriage return to display the shell prompt, the llogin will process continue to run, consuming all the free CPU time available.
Patch 300.00 OSF415-400377	**Patch:** Memory Leak With (dlb) Pseudodevice Driver **State:** Existing Fixes a memory leak problem that occurs with the STREAMS Data Link Bridge (dlb) pseudodevice driver. This problem could cause a "freeing free mbuf" panic when system memory is exhausted.

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

Patch 302.00 OSF415-400406	**Patch:** Security, (SSRT0495U) **State:** Existing A potential security vulnerability has been discovered, where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability.
Patch 312.00 OSF415-400416	**Patch:** who Command Correction **State:** Existing Fixes a problem that occurs when more than 140 users are logged on to a system and the who command is issued. If the output from the command is redirected or piped, the last several lines become corrupt.
Patch 317.00 OSF415-400422	**Patch:** screen Correction, (SSRT0296U, SSRT0494U) **State:** Supersedes patches OSF415-400189 (91.00), OSF415-400189B (167.00), OSF415-400189B-1 (167.01), OSF415-400313 (202.00) This patch corrects the following: • A potential security vulnerability has been discovered in BIND (Domain Name Service), where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability. • This patch corrects a problem where, if the FLAG bit is set in the IP header, screend incorrectly reports: ACCEPT: Not first frag, off 64
Patch 320.00 OSF415-400427	**Patch:** Security, (SSRT0490U) **State:** Existing A potential security vulnerability has been discovered, where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability.
Patch 322.00 OSF415-400429	**Patch:** pcnfsd Correction **State:** Existing This patch provides the followig bug fixes and performance enhancements: • When signals causing pcnfsd to terminate or when a SIGPIPE signal was not caught, pcnfsd would exit without producing a core file. • The pcnfsd authentication would cause crashes and memory corruption.
Patch 327.00 OSF415-400438	**Patch:** Segfaults In nm For C++ Compiler Correction **State:** Existing Fixes segfaults in nm for object files generated by the C++ compiler.
Patch 330.00 OSF415-400443	**Patch:** AdvFS Consolidated Patch **State:** Existing Fixes a problem that occurs on AdvFS systems. The chfsets function returns incorrect exit values and inappropriate error messages.
Patch 335.00 OSF415-400455	**Patch:** lex Command Correction **State:** Existing Fixes a problem with the lex command. Programs built with lex may exhibit various problems which only occur after the following warning: Maximum token length exceeded

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

Patch 337.00 OSF415-400457	**Patch:** pax tar And cpio Archive Handling Correction **State:** Supersedes patches OSF415-400258 (160.00), OSF415-400320 (231.00), OSF415-400374 (291.00) This patch corrects the following: • Fix pax's tar and cpio archive handling to allow file sizes greater than 4GB. • Fixes a problem with the tar "tv" command in reporting ownership on a file that had no legitimate owner at the time it was archived. Based on the position of the file in the archive, tar returned the owner of a previous file, or the values -973 for userid and -993 for groupid. • Fixes problem in which /usr/bin/pax : cpio -pl does not link files when possible, but copies them. • Fixes a problem with the tar and pax programs. These programs incorrectly append files to an existing archive and cause the file to become corrupt.
Patch 340.00 OSF415-400465	**Patch:** LSM volsave Command Correction **State:** Existing This patch fixes a problem with the LSM volsave command. The volsave command returns an exit status of 1 (failure), even when the LSM configuration is successfully saved.
Patch 345.00 OSF415-400473	**Patch:** DEC C Compiler Correction **State:** Supersedes patches OSF415-400149 (68.00), OSF415-400187 (90.00), OSF415-400257 (159.00) This patch corrects the following: • Fixes a DEC C compiler problem that occurred when compiling a structure tag whose length exceeded 256 characters. • This patch provides a new version of the DEC C compiler to fix QAR 49944. It fixes a problem that causes the compiler to generate incorrect code for switch statements whose expression is of type short or type char. The version of this fixed compiler is "DEC C V5.2-035". • Fixes three DEC C compiler problems: – Fixes "Assertion failure: Compiler internal error" compiler crash that occurs when compiling xemacs. – Fixes "Invalid expression" error with valid token-pasting macro. – Fixes "Fatal: memory access violation" compiler crash when the left side of a structure pointer operator (->) was not an lvalue. This case should produce a compiler error. • Fixes the following problems: – A compiler code generation problem that caused incorrect code for a left shift on a signed int when compiled in ANSI (-std or -std1) compilation modes. – A problem where a structure return temporary is not preserved until later used in an enclosing funtion call; originally reported in the comp.UNIX.osf.osf1 newsgroup. – A "GEM ASSERTION, Compiler internal error" problem when compiling a complex conditional expression with -O0.

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

Patch 347.00 OSF415-400478	**Patch:** DIGITAL UNIX LAT Correction **State:** Existing When printing using DIGITAL UNIX LAT (V4.0 or later) to a printer connected to a PC running Pathworks, "I/O error" is displayed and nothing is printed.
Patch 352.00 OSF415CDE-400013	**Patch:** Security, (SSRT0498U) **State:** Existing A potential security vulnerability has been discovered in 'libDtSvc', where under certain circumstances users may gain unauthorized access. DIGITAL has corrected this potential vulnerability.
Patch 354.00 OSF415CDE-400015	**Patch:** Security, (SSRT0431U, SSRT0525U) **State:** OSF415CDE-400008 (129.00) A potential security vulnerability has been discovered, where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability.
Patch 356.00 OSF415DX-400015	**Patch:** Security, (SSRT0435U) **State:** Supersedes patches OSF415DX-400006 (132.00), OSF415DX-400009 (157.00), OSF415DX-400011 (200.00) This patch corrects the following: • A potential security vulnerability has been discovered, where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability. • Fixes a problem that occurs on DIGITAL UNIX systems running Version 4.0 or higher with C2 security enabled and Patch OSF415DX-400006 installed. The dop command rejects all password attempts when run non-root users. • Fixes a problem that occurs on systems that have installed Patch OSF415DX-400006. If more than one argument is given on the dop command line, dop passes all arguments as a single argument to the command. • The startup of nissetup, latsetup and btcreate /etc/doprc entries via the dop command fails with exit code of 2.
Patch 357.00 OSF415-405127	**Patch:** Token Ring Transmission Timeout Correction **State:** Supersedes patches OSF415-405043 (34.00), OSF415-405043-1 (34.01) This patch corrects the following: • This patch fixes a Token Ring transmission timeout. The driver can experience "ID 380PCI20001 (8/13/95)" in the TI380PCI Errata on the AlphaServer 4100 platform. • An upgrade/replacement for the Token Ring driver. This patch fixes an intermittent kernel memory fault problem. To ensure data integrity, additional enhancements to transmit and receive list processing routines have also been added.
Patch 361.00 OSF415-405135	**Patch:** Alpha VME 4/2xx System Panic Correction **State:** Existing Fixes a problem that occurs on Alpha VME 4/2xx systems. The system may panic and display the following error message: kernel access memory fault

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

Patch 365.00 OSF415X11-405007	**Patch:** dtterm Displays All Characters in PC Codeset IBM-850 **State:** Supersedes patch OSF415-400468 (343.00) This patch corrects the following: • Provides a new en_US.cp850 locale for processing text data originating from the PC environment. • Provides the ability to let dtterm display all the characters in the PC codeset IBM-850.
Patch 372.00 OSF415-410127	**Patch:** Fatal System Information Not Displayed To Terminal **State:** Existing Fixes a problem that occurs when fatal system and processor machine check information is not displayed to the console terminal.
Patch 393.00 OSF415-410150	**Patch:** Provides filterlog For Improved Error Reporting **State:** Supersedes patch OSF415-410160 (401.00) This patch corrects the following: • Fixes a problem specific to the AlphaServer 8200/8400 in which the binary.errlog file becomes corrupt. The following error message is displayed: 620 System Correctable Error • Provides a new command, filterlog, which improves error reporting on AlphaServer 8200/8400 systems.
Patch 394.00 OSF415-410151	**Patch:** ASDU netbeui server connection closing **State:** Supersedes patches OSF415-410048 (11.00), OSF415-410090 (209.00), OSF415-410136 (377.00) This patch corrects the following: • STREAMS tty line discipline was not correctly processing type-ahead characters. • Fixes a wide variety of system panics and other problems caused by random memory corruptions. • The ASDU netbeui server (nbelink) will not close a connection. It will hang hang in dlcb_close awaiting a STREAMS event. Subsequently, new connecitons will not be able to connect to nbelink.
Patch 405.00 OSF415-405154	**Patch:** sort Command Correction **State:** Existing Fixes the error condition that the sort command may erroneously skip 8-bit characters when the -d or -i option is specified.
Patch 407.00 OSF415-405157	**Patch:** lpd Line Printer daemon **State:** Existing Fixes a problem with the lpd line printer daemon. When "/sbin/init.d/lpd stop" is followed right away by "/sbin/init.d/lpd start", the new lpd lpd fails to start. The error message from syslog is: /usr/spool/lpd.lock: locking failed: Operation would block

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

Patch 415.00	**Patch:** auth_for_terminal() Segmentation Fault Correction
OSF415-405165B	**State:** Supersedes patches OSF415-400115 (51.00), OSF415-400203 (100.00), OSF415-400203B (488.00) This patch corrects the following: • Under enhanced security, sometimes users (even root) are unable to log in on graphics console, even after using dxdevices or edauth to clear the t_failures count. • On systems running enhanced security, user-written applications that call auth_for_terminal() may fail with a segmentation fault. • A potential audit vulnerability has been discovered, where under certain circumstances, the audit trail of a user may be compromised. DIGITAL has corrected this potential vulnerability.

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

Patch 422.00 OSF415-405174	**Patch:** OTTO/OPPO ATM Driver Correction **State:** Supersedes patches OSF415-400253 (156.00), OSF415-400286 (181.00), OSF415-400411 (309.00), OSF415-400425 (319.00), OSF415-400432 (324.00) This patch corrects the following: • This patch is an upgrade/replacement for the OTTO/OPPO ATM driver and fixes a number of flow control and signalling problems. If you are seeing "No Buffer Space" messages, experiencing pauses or hangs when receiving data on signalling/ilmi pvc's, or have any problems with FLOWMASTER flow control with CLIP or LANE over ATM, you should install this patch. • Fixes two problems with the ATM 350 driver. – On reboot, a panic could be encountered before getting into single user mode. The panic would occur inside the ltaintr routine and this routine would be noted in the dump stack trace. This problem was seen on Personal Workstation 500ua (MIATA) and the ATM 350 card. – The second problem is a panic: thread_block: interrupt level call when rt_preempt_opt (REALTIME preemption) is enabled. A typical stack trace would look like this for the top of the stack: panic thread_block() thread_preempt() panic thread_block() unix_release_force() unix_release() schedtransmit() softclock_scan() Or this: panic thread_block() thread_preempt() panic thread_block() unix_release_force() unix_release() ottooutput() atm_cmm_send() • An upgrade enhancement to the ATM350 driver. This patch prevents panics in driver routines that can be called from different interrupt levels. • Fixes a panic from the ATM OTTO/OPPO driver.
Patch 436.00 OSF415-405193	**Patch:** Security, (SSRT0456U) **State:** Supersedes patch OSF415-400412 (378.00) This patch corrects the following: • A potential security vulnerability has been discovered, where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability. • The rpc.statd process would sometimes disappear without a trace. So the fix is to ignore SIGPIPEs (triggered by statd behaviour). Also, this patch catches and logs other signals that would otherwise make rpc.statd disappear without a trace.

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

Patch 446.00 OSF415-405208	**Patch:** FDDI fta Driver Correction **State:** Supersedes patches OSF415-400225 (115.00), OSF415-400409 (290.00), OSF415-400467 (342.00) This patch corrects the following: • An upgrade/replacement for the "FTA" FDDI driver and fixes a DMA Error which can occur with the older driver. If it became necessary to back out a partially constructed frame from the transmit queue, the older driver was unable to properly backed out the frame before restarting. This resulted in the following errors being logged to the /var/adm/messages file: vmunix: fta0: Halted. vmunix: fta0: Halt Reason: DMA Error. vmunix: fta0: Link Unavailable. vmunix: fta0: Link Available. • Fixes a problem that may occur on systems with a FDDI controller. During system boot, the system may panic with a message similar to the following: panic (cpu 8): kernel memory fault • Fixes a kernel memory fault caused by the fta FDDI driver. • Corrects a problem with the FDDI fta driver.
Patch 449.00 OSF415-405211	**Patch:** /sbin/loader Correction **State:** Supersedes patch OSF415-400152 (71.00) This patch corrects the following: • Fixes a problem that may cause /sbin/loader to fail to resolve duplicate symbols in dlopen'ed shared libraries. • Addresses two issues with the /sbin/loader. – Fixes an infinite loop in /sbin/loader. – Changes the /sbin/loader so that it now reports the names of unresolved symbols in a shared library which is opened by a dlopen() call.
Patch 454.00 OSF415-405218	**Patch:** ncheck Utility With -s Option On AdvFS File Systems **State:** Existing Fixes an AdvFS problem. When running the ncheck utility with the -s option on an AdvFS file system, the command never returns but instead justs keeps using CPU cycles. This problem only occurs when there are no special files in the file system.
Patch 460.00 OSF415-405227	**Patch:** mountd Correction, Security (SSRT0496U) **State:** Supersedes patches OSF415-400343 (241.00), OSF415-405201 (441.00) This patch corrects the following: • A potential security vulnerability has been discovered, where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability. • Fixes the mount command. An incorrect error message is displayed when trying to mount a directory, which does not exist, under a valid exported file system. • Fixes a problem in mountd where lines in the /etc/exports file could be no longer than 1023 characters. With this patch, a trailing backslash character in the /etc/exports file allows continuations beyond 1023 characters.

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

Patch 475.00 OSF415-405244	**Patch:** kdbx mbuf And socket Extensions Correction **State:** Existing Corrects a problem with the kdbx mbuf and socket extensions. The use of these extension on some crashdumps resulted in errors and would hang.
Patch 477.01 OSF415-405248-1	**Patch:** Run-Time Support For DIGITAL C++ V6.0 Compiler **State:** Supersedes patch OSF415-400487 (349.00) The required run-time support for images created by the DIGITAL C++ V6.0 and above compiler. Contact the DIGITAL C++ compiler group (cxx@lego.zko.dec.com) for details.
Patch 481.00 OSF415CDE-405003	**Patch:** dtbuilder Core Dump Correction **State:** Supersedes patch OSF415CDE-400010 (165.00) This patch corrects the following: • The application builder (dtbuilder) core dumps when changing the default button in the revolving property editor. • Fixes a segmentation fault in dtbuilder that occurs when a user tries to generate code using a 'When: Dragged From' action in conjunction with the 'list' object type.
Patch 482.00 OSF415CDE-405004	**Patch:** xset Command Correction **State:** Existing Fixes a problem where the xset command could not clear the screen saver under CDE.
Patch 485.00 OSF415X11-405008	**Patch:** Memory Leak In X server Processing ListExtensions() **State:** Existing Fixes a memory leak in the X server when processing ListExtensions() requests. This problem is seen in particular on systems with a PowerStorm 4D51T graphics card.
Patch 489.00 OSF415-400362B	**Patch:** libm Static Library Correction **State:** Supersedes patches OSF415-400083 (46.00), OSF415-400293 (185.00), OSF415-400362 (250.00) This patch corrects the following: • Fixes the problem of the math library functions not returning the correct NaN value as defined in the *Alpha AXP Architecture Reference Manual* (Second Edition). • Fixes a problem with fastmath functions F_Exp() and F_Pow() that would cause floating exception core dumps.
Patch 492.00 OSF415-400365B	**Patch:** btree File Format Correction **State:** Supersedes patch OSF415-400365 (252.00) Fixes a probem that affects systems using databases with the btree file format. Only applications using btree in libdb.a or libdb.so are affected and may return incorrect data or crash.
Patch 493.00 OSF415-405248B	**Patch:** Run-Time Support For C++ V6.0 Compiler, Static Lib **State:** Supersedes patches OSF415-400487 (349.00), OSF415-405248 (477.01) The required run-time support for images created by the DIGITAL C++ V6.0 and above compiler. Contact the DIGITAL C++ compiler group (cxx@lego.zko.dec.com) for details.

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

Patch 494.00 OSF415CDE-400006B	**Patch:** Nodename Length Correction, Development **State:** Supersedes patch OSF415CDE-400006 (127.00) This patch fixes a problem in which users logging into a system that has a nodename longer than 32 characters cause ttsession to core dump. This only happens when using CDE desktop.
Patch 496.00 OSF415-400371B	**Patch:** uprofile, kprofile Command Corrections, Development **State:** Supersedes patch OSF415-400371 (259.00) This patch corrects the following: • The uprofile and kprofile commands report incorrect statistics on an SMP system or when trying to measure EV5 events other than cycles. • The pfm driver ioctl PCNT5GETCNT returns incorrect data. • An unstoppable stream of pfm interrupts is produced if an EV5 machine is rebooted with the pfm driver active. • The pfm(8), uprofile(1), and kprofile(1) manpages do not describe the EV5 statistics supported by the software. All users of the pfm driver and uprofile or kprofile commands should install this patch.
Patch 498.00 OSF415-410042-1	**Patch:** S3 Trio64V+ Graphics Card Incorrectly Identified **State:** Supersedes patch OSF415-410042 (8.00) The S3 Trio64V+ graphics card is not being correctly identified by the driver at startup.
Patch 499.00 OSF415CDE-405010	**Patch:** Problems with CDE Calendar Manager **State:** New Fixes the following problems with the CDE Calendar Manager: • The calendar manager service daemon (rpc.cmsd) core dumps when processing a calendar database file containing invalid entries. • Repeating appointments with a frequency of daily are sometimes displayed incorrectly by the calendar manager (dtcm). • The calendar manager (dtcm) will complain that it cannot connect to the calendar manager service daemon (rpc.cmsd) and rpc.cmsd will repeatedly start and die with constantly changing pids.
Patch 500.00 OSF415CDE-405011	**Patch:** dtmail Command Core Dumps **State:** New Fixes a problem where dtmail can core dump when there exists long lines in Sun Mail Tool attachments. This causes a buffer overflow.
Patch 501.00 OSF415CDE-405005	**Patch:** dxkeyboard Application Modification **State:** New Installs a modified dxkeyboard application that correctly loads the XKB keymap for the Hebrew LK401 keyboard so that the Ctrl+Hebrew toggle key works in a DECterm window.

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

Patch 502.00 OSF415CDE-405006	**Patch:** CDE Window Manager Correction **State:** Supersedes patch OSF415CDE-400005 (126.00) This patch corrects the following: • Fixes two problems with the CDE window manager. In the first problem, the CADDS5 (a third party cad tool) text window tends to walk off the screen. In the second problem, the CDE icon box moves 29 pixels higher along the x axis each time the user's home session is resumed. • Fixes a problem in which deleting applications (icons) from some subpanels hangs the CDE Window Manager. The subpanels affected are "Calendar", "Mail" and "Desktop Style" subpanels.
Patch 503.00 OSF415CDE-405007	**Patch:** Security (SSRT0438U) **State:** Supersedes patch OSF415CDE-400007 (128.00) This patch corrects the following: • A potential security vulnerability has been discovered, where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability. • Fixes a problem in which the CDE file manager (dtfile) fails to open files that use dtpad as the exec'd action. This includes both double-clicking on the file and using 'Open' from the 'Selected' pulldown menu.
Patch 504.00 OSF415CDE-405008	**Patch:** CDE dtterm Correction **State:** Supersedes patches OSF415CDE-400004 (125.00), OSF415CDE-400012 (351.00), OSF415CDE-400014 (353.00) This patch corrects the following: • Users appear to be logged in when they are not because CDE dtterm sometimes doesn't reset the utmp entry on exit. • When running the Common Desktop Environment (CDE), a dtterm window in which vi is being used can hang when doing a cut and paste operation from a second window. • Provides the ability to let dtterm display all the characters in the PC codeset IBM-850. • Fixes a problem in which the dtterm Terminal Emulator fails to send the "DO" and "HELP" User Defined Keys when depressed. It also fixes a problem in which proper escape sequences for "F10", "DO", and "HELP" were not being reported when the keys were depressed.
Patch 505.00 OSF415CDE-405009	**Patch:** CDE Calendar Manager Hangs **State:** New Fixes a problem where the Common Desktop Environment (CDE) calendar manager (dtcm) will hang if you enter an appointment 25 days or more in advance when there are no intervening appointments.

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

Patch 509.00	**Patch:** Account Management Command Corrections
OSF415DX-405008	**State:** New. Supersedes patches OSF415DX-400005 (131.00), OSF415DX-400008 (134.00), OSF415DX-400010 (190.00), OSF415DX-400013 (355.00), OSF415DX-405003 (483.00), OSF415DX-405004 (484.00), OSF415DX-405005 (506.00), OSF415DX-405006 (507.00), OSF415DX-405007 (508.00) This patch corrects the following: • When creating a new user account with a home directory of root, the permissions on the root directory are changed to 700, rendering the root file system inaccessible to non-root users. • Patch Kit-0001 causes a problem with the System V Environment (SVE) /usr/opt/svr4/usr/bin/passwd command. If an invalid password is entered, subsequent invocations of the passwd command, /usr/bin/X11/dxaccounts command, or the account management commands fail with the following error: The password and group files are currently locked by another user. • Fixes for miscellaneous problems with the account management commands, specifically the Account Manager graphical user interface (/usr/bin/X11/dxaccounts) and the command line interface (useradd, userdel, groupadd, etc). • Fixes a problem that causes the account management commands (dxaccounts, useradd, and usermod) to split long NIS group lines incorrectly. This causes a majority of users to have improper access to files, directories, and applications and also causes the newgrp command to fail. • Fixes the following problems: – When Enhanced Security is enabled, the useradd and usermod commands incorrectly set the password expired and password lifetime attributes to 0 when not specified on the command line. – The administrative_lock_applied command line option for useradd and usermod does not correctly lock and unlock an account. – The administrative_lock_applied command line option for useradd and usermod does not correctly lock and unlock an account. • When issuing a useradd -D or usermod -D command to view the account manager defaults, the Inactive (days) value would always show the character 's' rather than nothing when the Inactive days status has been defeated with a -1 value. • Fixes the following problems encountered when using the Account Manager application (dxaccounts): – When modifying an existing NIS "+" or NIS "-" user account by turning off the NIS Overrides toggle, the User ID field is incorrectly set to 0. – While adding a NIS "+" or NIS "-" user, dxaccounts requires a password to be set. • Fixes a problem where Dxaccounts allows the ':' character to be accepted in the user shell, home directory, fullname, office, office phone, and home phone fields. This caused the /etc/passwd file to become corrupted.

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

Patch 509.00 continued	• Fixes a problem using templates for preexpired passwords. When the administrator creates a template and within the template chooses force password change at the next login, the user is NOT being asked to change his password as he should. • Fixes the problem where usermod -g will lock the user account if it is unlocked. • Fixes a problem where the account manager graphical interface (dxaccounts) will core dump on systems running enhanced security when performing a "Find Local User..." or "Find NIS User..." operation in which "Secondary Groups" is the only search criteria that has been specified.
Patch 510.00 OSF415DX-405009	**Patch:** Fix for dxdiff Core Dump **State:** New Fixes a problem where dxdiff will core dump when comparing files with long lines.
Patch 518.00 OSF415-405258	**Patch:** FDDI Memory Leak Correction **State:** Supersedes patches OSF415-400275 (178.00), OSF415-400330 (236.00), OSF415-405186 (432.00) This patch corrects the following: • Fixes memory leaks with the FDDI and Token Ring method routines used with Extensible SNMP subagent (ESNMP). • The SNMP agent returns incorrect data when requested for the MIB II Address Translation Table (atTable). The agent returns correct data for ipNetToMediaTable, which supersedes atTable in MIB II. This patch removes support for atTable, so that common applications (like NetView autodiscovery) will use the ipNetToMediaTable instead. • Fixes the os_mibs source file, hrm_fs.c, which makes a call to the statfs function with 2 arguments, when statfs expects 3 arguments. • Fixes the problem where a malformed trap message sent at boot-time by the DIGITAL UNIX SNMP daemon to a Windows NT Network Management Station (NMS) could cause the NMS application or the NT operating system to crash.
Patch 523.00 OSF415-405266	**Patch:** linker Problem Printing Lengthy Error Diagnostics **State:** Supersedes patches OSF415-400174 (84.00), OSF415-400375 (258.00), OSF415-405212 (450.00) This patch corrects the following: • Fixes a problem where use of "ld -r" will change symbol preemption behavior. • Fixes four linker problems: Hidden/export symbols, Assert getting generated with R_GPVALUE relocations, improper Text segment alignment processing, and linker memory management problem processing C++ symbols. • Fixes a problem where the linker might crash when printing out lengthy error diagnostics. • Fix for a linker problem that could cause incorrect symbol resolution in call_shared applications. The result is the application may use a shared library's version of a symbol rather than a symbol with the same name defined in the application.

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

Patch 527.00 OSF415-405273	**Patch:** AdvFS Boot Correction **State:** New Fixes a problem in which AdvFS boot code has trouble traversing symbolic links.
Patch 532.00 OSF415-405279	**Patch:** ftp Command Correction, (SSRT0505U) **State:** Supersedes patches OSF415-400144 (65.00), OSF415-400150 (69.00), OSF415-400396 (306.00), OSF415-405161 (410.00), OSF415-405188 (433.00) This patch corrects the following: • Fixes a problem with the ftp command. If you ftp to an IBM MVS system using the IP address, the IBM system will refuse the connection. This problem can be encountered on any system that validates TOS (Type Of Service) requests if the file /etc/iptos is not used on the client. • 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. DIGITAL has corrected this potential vulnerability. • Fixes hang conditions experienced with the following networking commands and utilities rsh(1) telnet(1) ftp(1) rdate(8) ping(8) and yppush(8). • Corrects a regression problem with the rsh(1) command. • Corrects a problem with rsh(1) that is most visible with long-distance (slow) links where a packet might get dropped.
Patch 539.00 OSF415-405290	**Patch:** last Command Fix **State:** New Fixes a problem with the last(8) command. Users that have logged out of a system are still listed as active in the /var/adm/wtmp accounting file.

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

Patch 541.00 OSF415-405294	**Patch:** LAN Emulation Client LANE V1 Compliance **State:** New. Supersedes patches OSF415-400138 (61.00), OSF415-400219 (112.00), OSF415-400288 (182.00), OSF415-400464 (339.00), OSF415-405158 (408.00), OSF415-405163 (412.00), OSF415-405164 (413.00), OSF415-405183 (429.00), OSF415-405225 (458.00), OSF415-405234 (466.00), OSF415-405220 (456.00), OSF415-405261 (520.00) This patch corrects the following: • Fixes problems in the error paths of the ATM subsystem. A majority of these result in system crashes. These crashes are most prevalent when stressing LAN Emulation (LANE). • Fixes two panics in the lta driver, ATM LANE interoperability problems with IBM switches, and slow recovery of UNI 3.0 signalling from network interruptions. • When tcpdump is run with ATM LAN emulation, a kernel memory fault occurs. • Fixes a problem with the ATMworks 351 (Meteor) loadable driver. • Fixes an ATM problem. When the ATM subsystem receives a CONNECT message with no signalling information elements (IEs), it corrupts a single byte of kernel memory. • Fixes a problem when ATM ELAN's are configured and an ATM switch reboots. This can cause a temporary connectivity problem. Hosts on Ethernet segments may not be able communicate with the DIGITAL UNIX ATM ELAN hosts until the expiration of router ARP timers. • Fixes a problem that occurs on a system running ATM. The system panics with a "kernel memory fault" due to a simple lock time violation. Prior to the crash, the pvc flag is observed as stale on a permanent virtual circuit. The crash occurs after the pvc is deleted with the following command: # atmconfig -pvc ..... • Fixes the conformance problem with the DIGITAL UNIX LAN Emulation. The DIGITAL UNIX LAN Emulation client now complies with the LANE V1 spec when locating the LAN Emulation Configuration Server (LECS). The client now asks the switch via ILMI for the ATM address of the LECS. • ATM will fail to connect on incoming calls that are UNI version 3.1 In some cases incorrect data for the Elan name was being used. This would cause D/UNIX to try to join an invalid Elan. • This fix allows the "elan_name" option to be set with the "les" option. • Fixes two problems in ATM. A Virtual Circuit may hang when running Classical IP under a very heavy load, and the kernel malloc pool could be corrupted, causing kernel memory faults. • Fixes a problem in which an ATM CLIP connection does not send data. • Fixes an interoperability problem with CISCO CLIP clients.

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

Patch 542.00 OSF415-405295	**Patch:** Enhancements to Print Services **State:** Supersedes patch OSF415-400290 (184.00) This patch corrects the following: • Fixes a problem where the lpq command causes the program to crash (Memory fault). • Contains many fixes to improve the reliability and efficiency of DIGITAL UNIX print services.
Patch 545.00 OSF415-405300	**Patch:** find Command Correction **State:** Supersedes patch OSF415-400379 (307.00) This patch corrects the following: • Fixes various problems with the find command. • Fixes the "find" command in which files in directories which were mounted with the "-fstype nfsv2" argument were not found.
Patch 552.00 OSF415-405311	**Patch:** mailx Command Correction (SSRT0758U) **State:** Supersedes patch OSF415-400172 (83.00) This patch corrects the following problems: • Fixes two problems with the mailx command. • 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. DIGITAL has corrected this potential vulnerability.
Patch 555.00 OSF415-405315	**Patch:** kloadsrv May Cause System Panic **State:** Supersedes patch OSF415-400243 (152.00) This patch corrects the following: • Fixes a problem in which loadable kernel modules that are loaded with the kloadsrv daemon at run time, may cause a system panic. • Ensures that kloadsrv remains running when the system is shut down to the single user run level.

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

Patch 561.00 OSF415-405327	**Patch:** ex and vi Editor Corrections **State:** Supersedes patches OSF415-400204 (101.00), OSF415-400390 (289.00), OSF415-410114 (297.00), OSF415-410121 (368.00) This patch corrects the following: • This patch fixes several problems in the ex and vi editors. – Blank lines in the .exrc file prevent the vi editor from executing. – The ex editor does not properly manage the file name buffers when a "write append" command fails. – The vi editor may erroneously report a "Bad file number" error message when switching between files. • Fixes a problem in which the vi command, "ce", does not work as expected. • Fixes a problem that causes the vi command to core dump. The problem occurs if one line is yanked into a named buffer. For example, the following command, which should mark the current line and copy the line into buffer "a", will generate a core dump: may'a • Fixes a problem in which the vi command, "ce", does not work as expected. • Fixes a problem with the vi editor envrionment variable EXINIT that occurs when EXINIT includes the editors so subcommand.
Patch 562.00 OSF415-405328A	**Patch:** acctcom Command Correction **State:** Supersedes patch OSF415-400230 (119.00) This patch corrects the following: • Fixes a problem in which the size field of a process displayed by the acctcom command is displayed incorrectly. • Corrects a small accounting problem where the measured time for a process was an integral rather than mean value.
Patch 563.00 OSF415-405329	**Patch:** tip Command Correction **State:** New. Supersedes patch OSF415-405264 (522.00) This patch corrects the following: • Fixes a problem with the tip command. A user can not escape to a local shell from tip when using csh. • A potential security vulnerability has been discovered in the 'tip' command, where under certain circumstances users may gain unauthorized access. DIGITAL has corrected this potential vulnerability.
Patch 568.00 OSF415-405336	**Patch:** LEX Correction **State:** Supersedes patch OSF415-400177 (86.00) This patch corrects the following: • Fixes a LEX problem. Without this patch, LEX rejects quoted regular expressions where the ending quote is preceded by a double backslash backslash, as in: "\\"xxx, and produces the following message: "lex:(Warning at line 8)Non-terminated string" • Fixes a problem in lex that causes it to not recognize the end of a comment when the final "/" is preceded by more than one consecutive "*".

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

Patch 569.00 OSF415-405337	**Patch:** Security, (SSRT0487U) **State:** Supersedes patch OSF415-400404 (301.00), OSF415-405233 (465.00) This patch corrects the following: • A potential security vulnerability has been discovered, where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability. • Fixes the following problems with the "at -t" command: – The command did not work with user id's that were not in the password file. – The command did not work on the leap year of 2000. • Corrects several problems with the "at", "cron", and "crontab" commands.
Patch 570.00 OSF415-405338	**Patch:** Line Printer Performance Fix **State:** New Fixes a problem with the performance of some line printers on a 4100 cpu.
Patch 576.00 OSF415-405346	**Patch:** Machine Server System Call Incorrect Type Check **State:** New Fixes a problem where the machine server system calls are not being type checked properly potentially causing system crashes by unprivileged programs.
Patch 580.00 OSF415-405353	**Patch:** dd Command Correction **State:** Supersedes patches OSF415-400211 (105.00), OSF415-400211-1 (105.01), OSF415-400211-2 (105.02), OSF415-405195 (437.00) This patch corrects the following: • Fixes a problem in which the dd command can corrupt output on very large files (2GB or greater) when the "conv=sparse" option is used. • Fixes a problem that occurs with the dd command. When the seek option to the dd command is used to insert data into an existing output file, the resulting file is incorrect and all of the original data is lost. • Fixes a problem with the dd command in which dd aborts after a read error. This problem occurs even when the "conv=noerror" parameter is specified.
Patch 584.00 OSF415-405359	**Patch:** advscan Data Corruption Fix **State:** New. Supersedes patch OSF415-405263 (521.00) This patch corrects the following: • Fixes a problem caused by the advscan -r command. The command would link LSM volumes to the raw device instead of the block device when it attempted to recreate LSM volume links. As a result, the directory for the domain name in the /etc/fdmns file was incorrect and data corruption occurred. • Fixes a problem in which the "advscan -a" command causes a memory fault (core dump) while processing LSM volumes.

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

Patch 585.00 OSF415-405360	**Patch:** expr Command Correction **State:** New Fixes a problem with the expr command in which the leading zeros are truncated if CMD_ENV is set to bsd.
Patch 586.00 OSF415-405361	**Patch:** faa FDDI Driver Kernel Memory Fault Correction **State:** New. Supersedes patches OSF415-400280 (179.00), OSF415-405196 (513.00) This patch corrects the following: • Fixes a kernel memory fault caused by the faa FDDI driver. The panic was due to incomplete handling of an error condition by the driver ("Timeout in command request"). The command request buffer was freed, however the reference to it was not removed from the command request list. When this list was later accessed, the invalid memory reference panic occurred. • Fixes a kernel memory fault in faa_service_rcv_q() in the faa FDDI driver. • Fixes a problem in which a system with a FutureBus+ FDDI adapter experiences problems when a command issued to the adapter fails.
Patch 593.00 OSF415-405369	**Patch:** rpc.lockd Correction **State:** Supersedes patches OSF415-400246 (154.00), OSF415-405178 (426.00) This patch corrects the following: • Fixes several problems with the network lock daemon, rpc.lockd: – NFS mounted file systems may hang. – The rpc.lockd program may fail because it loses a message granting NLM approval. – The rpc.lockd daemon may crash with a core dump. – An error occurs with NFS mounted user mail files. This error prevents the files from being locked and prints out the following message: cannot lockf – An NFS problem may occur. The system displays the following error message: NFS error 48 cannot bind sockets • Addresses various rpc.lockd problems. • Corrects two problems, the first change moves locked files from the message queue to the held list once. The second change adds code to allow locked files leftover from a server reboot, to timeout and be transmitted to the server.
Patch 594.00 OSF415-405370	**Patch:** Process Hang When Calling flock **State:** New Fixes a problem that can cause calls to flock() to hang a process on an SMP system if two or more processes are attempting to obtain and release an flock() on the same file.

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

Patch 596.00 OSF415-405372	**Patch:** rdist Utility Correction **State:** Supersedes patch OSF415-400424 (318.00) This patch corrects the following: • Fix for rdist utility to prevent segmentation fault. • Fixes a problem where rdist dumps core when trying to copy a partition using the rdist command.
Patch 597.00 OSF415-405374	**Patch:** automount daemon Correction **State:** New Fixes an automount problem. An automount map file entry that included a comment was being parsed incorrectly, resulting in an error.
Patch 598.00 OSF415-405375	**Patch:** rmfdmn Command Fix **State:** New. Supersedes patch OSF415-405314 (554.00) This patch corrects the following: • Fixes a problem with the rmfdmn command, which previously displayed success messages on the standard error device instead of the standard output device. • Fixes a problem with the rmfdmn command. The command would fail when it attempted to rename the domain to be deleted, so the domain was not deleted. However, the command returned success for the operation.
Patch 599.00 OSF415-405376	**Patch:** ddr_config Corrections **State:** Supersedes patches OSF415-400066 (43.00), OSF415-400218 (111.00), OSF415-400218-1 (111.01), OSF415-020 (171.00) This patch corrects the following: • DDR subsystem updated to handle SCSI devices returning a non-standard device type. • Fixes two problems with ddr_config. ddr_config previously would sometimes build partial device records. ddr_config on DIGITAL UNIX V4.0 was not compatible with input files created prior to this version. • Adding device recognition for TZS20. • Fixes a problem in which the DDR database (/etc/ddr.dbase) limited the maximum block size of "unknown" tape drives to 64 kilobytes. The maximum block size is changed to 16 megabytes.
Patch 600.00 OSF415-405377	**Patch:** Pseudo TTY Corrections **State:** Supersedes patches OSF415-400092 (47.00), OSF415-405042 (33.00) This patch corrects the following: • Fixes a problem that causes the system to "assert_wait" panic and the stack contains streams modules. • A problem where a remote user will kill rlogin or telnet and the server host will have an orphanned login process and rlogind or telnetd process in sleep state indefinitely. This is seen only with Asian tty (atty) or any other host which is running c-list rather than STREAMS tty's. • Fixes a panic caused by freeing a pty on a reopen of the controlling tty.

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

Patch 604.00 OSF415-405382	**Patch:** showfile Cmd Incorrectly Returns Error Status **State:** New Fixes a problem with the showfile command, which incorrectly returned an error status when it attempted to display a file that was a symbolic link.
Patch 608.00 OSF415-405387	**Patch:** cron Command Correction **State:** Supersedes patch OSF415-400194 (94.00) This patch corrects the following: • Fixes a problem in which the cron command deletes non-local file system files mounted in either the /tmp, /var/tmp, or /var/preserve directories. • Prevents the crontab file from incorrectly deleting files found in file systems mounted under the /var/preserve, /tmp, and /var/tmp directories.
Patch 610.00 OSF415-405390	**Patch:** diskx Cmd Fails with Data Validation Errors **State:** New This patch corrects the following: • Fixes a problem in which the /usr/field/diskx command fails with data validation errors when specifying a block device special file for testing. • This patch also provides diskx with the ablity to test 9 Gigabyte drives and provides added flexibility in diagnosing hardware problems.
Patch 614.00 OSF415-405395	**Patch:** Security (SSRT0448U, SSRT0452U) **State:** Supersedes patches OSF415-400167 (78.00), OSF415-400428 (321.00) This patch corrects the following: • A potential security vulnerability has been discovered, where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability. • Fixes a problem with the ftp daemon, ftpd, and its use of authenticated user information. The daemon was using incorrect information for logging and validation of usernames.
Patch 620.00 OSF415-405406	**Patch:** Security, sendmail (SSRT0421U) **State:** Supersedes patch OSF415-400160 (75.00) This patch corrects the following: • A potential security vulnerability has been discovered with the sendmail command, where under certain circumstances, users may gain unauthorized access. DIGITAL has corrected this potential vulnerability. • Fixes a problem with the sendmail program. Sendmail would dump core and not process any more jobs in the queue when it encountered control characters in a qf file.
Patch 621.00 OSF415-405407A	**Patch:** setacl Correction **State:** New Corrects the problem with setacl not being able to handle a user ID beginning with a numeral.

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

Patch 622.00 OSF415-405408	**Patch:** Unclear AdvFS Message **State:** New. Supersedes patch OSF415-405320 (557.00) This patch corrects the following: • Fixes a problem with an unclear AdvFS message. When trying to mount an AdvFS fileset on a system that did not have AdvFS installed, the following message was displayed: No such device Now, in similar cases, the following AdvFS message is displayed: Cannot mount AdvFS fileset, AdvFS not installed • Fixes a problem with AdvFS and links in the /etc/fdmns directory. Previously, AdvFS did not ensure that every link in a directory entry pointed to a block device. Now, it does.
Patch 623.00 OSF415-405411A	**Patch:** clock_settime Correction **State:** Supersedes patch OSF415-400215-1 (107.01) This patch corrects the following: • When setting the date with the clock_settime rtl service routine, the date will not get past the date of 'Sat Sep 8 19:46:39 2001'. If you try to set past this date the routine returns a EINVAL error. • Fixes the following two problems with realtime library: – A locking problem when calling sem_close() with an invalid descriptor – A memory leak
Patch 624.00 OSF415-405412	**Patch:** Simple Lock Time Limit Exceeded Panic **State:** Supersedes patch OSF415-400255 (158.00) This patch corrects the following: • Fixes a problem that occurs on SMP systems using LSM in which the system panics with a "simple lock time limit exceeded" message. • Fixes a problem in lsm. A data corruption occurs when readv/writev coallesced via physio while in read/writeback mode.
Patch 627.00 OSF415-405418	**Patch:** dbx Correction **State:** New. Supersedes patches OSF415-400205 (102.00), OSF415-405257 (517.00), OSF415-405413 (625.00) This patch corrects the following: • This patch fixes a problem that causes dbx to hang when stepping past a system() function call. • Fixes a dbx problem with listing a large Fortran program that contains alternate entry points. • Fixes a problem with dbx when debugging programs that have large source files. In some cases dbx may abort with a segmentation fault. • Fixes a problem with dbx. A segmentation fault may occur when displaying an array or when showing the type and dimensions of an array.

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

Patch 634.00 OSF415-405432	**Patch:** Streams Device Handling Corrections **State:** Supersedes patches OSF415-405023 (30.00), OSF415-400146 (66.00), OSF415-400236 (147.00), OSF415-400324 (233.00) OSF415-400368 (254.00), OSF415-405184 (430.00) This patch corrects the following: • Fixes "kernel memory fault" panics from the kernel malloc() routine when System V FIFOs created via STREAMS and fattach() are in use. • Fixes a problem that causes the system to panic with a kernel memory fault or "malloc_audit: guard space corruption" with osr_run as an entry in the stack. • Prevents delivery of data in subsequent streams messages with one read of a streams pipe. This problem only happens if the read has a message length greater than the length of the first message in the pipe. • Fixes a problem that occurs when running STREAMS. The system panics with a kernel memory fault in either osr_run() or osr_reopen(). • Fixes the problem of a system hang due to corruption of a STREAM synchronization queue's forward pointer. The system hangs in the csq_cleanup() function. • Fixes a problem in the streams code which could have resulted in data corruption. • This patch fixes a problem in which the system panics with one of the following error messages: simple_lock: uninitialized lock simple_lock_terminate: lock busy
Patch 635.00 OSF415-405433	**Patch:** Handling Of High Numbers Of Interrupts **State:** Supersedes patch OSF415-405246 (476.00) This patch corrects the following: • Fixes a problem on DIGITAL's 8200/8400 machines where CPUs may be bombarded with interrupts. The high amount of interrupts may cause simple lock timeouts and kernel memory faults. • Fixes the following problems found on Alphaserver 8400/8200 class machine: – A system hang or error messages being printed to the console. This is seen when a loadable driver is unloaded. – A pcia error system panic or machine check.

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

Patch 637.00 OSF415-405436	**Patch:** Security, (SSRT0476U) **State:** Supersedes patches OSF415-405080 (211.00), OSF415-405128 (358.00), OSF415-410147 (392.00) This patch corrects the following: • Applications running System V pseudoterminal slave pty can hang forever on open() system call. • A potential security vulnerability has been discovered, where under certain circumstances, a kernel memory fault panic may occur. • A call to the select() system call may hang or incorrectly indicate that there is a message waiting from a terminal when there is nothing there. • Fixes a problem in which the system may panic with the following error message "kernel memory fault".
Patch 640.00 OSF415-405440A	**Patch:** Mutex Lock Problem in TLI (Static Library) **State:** New. Supersedes patches OSF415-400171 (82.00), OSF415-400196 (96.00), OSF415-400264 (173.00), OSF415-400151 (70.00), OSF415-400385 (308.00), OSF415-400405-1 (310.01), OSF415-405237 (514.00) This patch corrects the following: • Fixes a mutex lock problem in TLI. The problem causes multithreaded TLI applications to block forever. • Fixes the problem of t_optmgmt() T_NEGOTIATE calls returning T_SUCCESS, but not actually negotiating the socket options. This behavior is a UNIX95 specification standard compliance bug. • Fixes a problem that manifests itself by the system hanging or becoming inoperable when a number of XTI connections reaches 500. • Resolves a hang in the xticlose() routine and a kernel memory fault in the xti_discon_req() routine. • Corrects a problem with the xti/streams interface module which could result in a kernel memory fault panic during use by xti application programs. • Fixes a problem with the implementation of the TPI interface. This problem occurs if you are using DIGITAL's XTI libxti library with a third-party (non-DIGITAL) STREAMS driver. • Fixes a problem that occurs on a system when running STREAMS. The system panics with the following error message: "kernel memory fault" • Fixes libtli/libxti to correctly handle a continuation data message still on the stream head.
Patch 644.00 OSF415-405445	**Patch:** route_output() Memory Alloc. Correction **State:** New. Supersedes patch OSF415-405442 (641.00) This patch corrects the following: • Corrects a potential problem in the handling of a write() system call to a routing socket. • Fixes a routing corruption that could been seen as a kernel memory fault or a corruption within the 128 byte kernel memory bucket.

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

Patch 645.00 OSF415-405447	**Patch:** config Command Core Dumps **State:** New Fixes a problem in which the kernel build config command (obj/alpha/kernel/bin/config) core dumps if the fopen function fails.
Patch 647.00 OSF415-405449	**Patch:** Bourne Shell Performance Fix **State:** New Fixes a problem where the performance of the Bourne shell may be slow when there are many automounted directories in the search path (as defined by the PATH environment variable).
Patch 649.00 OSF415-405451	**Patch:** Audit Records Generated Incorrectly **State:** New Fixes a problem in which audit records are generated for selected operations against objects that are not in the filesystem.
Patch 650.00 OSF415-405453A	**Patch:** libcurses Shared Library Fix **State:** New Fixes a problem with the curses library. The infocmp command dumped core because two curses terminal capability tables were out of sync with each other.
Patch 651.00 OSF415-405454	**Patch:** EISA Bus Handling Corrections **State:** Supersedes patch OSF415-400170 (81.00) This patch fixes three problems that occur on systems with an EISA bus: • A system running four DE425 adapters off an EISA bus may hang. • If a device's EISA configuration file contains a function DISABLE keyword and the DISABLE option is selected, the device's driver may not be configured and probed at bus configuration time. • Fixes a problem in which EISA/ISA buses do not correctly match functions for loadable drivers. EISA configuration code returns a non-null Function_Name field for the token ring card. This field is ignored if the driver is configured statically. However, when configured dynamically, scan_eisa_slot attempts to exactly match whatever is specified in the sysconfigtab entry with what is returned by the token ring card.
Patch 654.00 OSF415X11-405010	**Patch:** Motif Toolkit Correction **State:** Supersedes patches OSF415X11-400015 (145.00), OSF415X11-400020 (264.00), OSF415X11-405009 (486.00) This patch corrects the following: • Fixes the following problem in the Motif toolkit. The drag-n-drop operation fails, which may cause Motif applications to abort. • Fixes the memory leak in the Motif text widget when changing colors using XtVaSetValues(). • Fixes a small memory leak in the Motif text widget. • Fixes the Motif tear off menu core dump problem. The problem is seen when the tear off menu from a pulldown menu is closed/destroyed.

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

Patch 655.00 OSF415X11-405011B	**Patch:** Security (SSRT0422U, SSRT0547U) **State:** Supersedes patches OSF415X11-400017 (201.00), OSF415X11-400021 (275.00) This patch corrects the following: • A potential security vulnerability has been discovered, where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability. • Fixes a memory leak in Xlib when using fonts in an international (I18N) environment. This problem affects Netscape Navigator in particular. • A potential security vulnerability has been discovered where under certain circumstances users may gain unauthorized access. DIGITAL has corrected this potential vulnerability.
Patch 657.00 OSF415X11-405013	**Patch:** Screen Flickers In Power_Save Mode Correction **State:** New. Supersedes patches OSF415X11-400013 (143.00), OSF415X11-405012 (656.00) This patch corrects the following: • Screen flickers on and off when in power-save mode. • Fixes a problem where the X server may generate a core dump during shutdown on a dataless management services (DMS) client system. • Fixes a problem that prevents an X server from starting. The following error message is displayed: Fatal server error: Cannot establish any listening sockets. Make sure an X server isn't already running.
Patch 658.00 OSF415DX-410004	**Patch:** svrServer_mib Correction **State:** New Corrects the following error message seen in the daemon.log file: svrSystem_mib[1434]:svrSystem_mib **ERROR esnmp_poll.c line 685: Method routine returned invalid status:2
Patch 661.00 OSF415-410166	**Patch:** AlphaStation 255 Hang Or Crash On Reboot **State:** Supersedes patch OSF415-410140 (388.00) This patch corrects the following: • Fixes a problem in which the AlphaStation 255 will either hang or crash when the system is rebooted. • Fixes a problem with the KZPAA driver not recognizing an optical jukebox.
Patch 667.00 OSF415-410174	**Patch:** AlphaServer 1000A 4/233 and 4/266 System Panic Fix **State:** New Fixes a problem on AlphaServer 1000A 4/233 and 4/266 systems where correctable memory error handling causes a system panic with a kernel memory fault.

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

Patch 673.00 OSF415-410188	**Patch:** Default C Compiler Correction **State:** New. Supersedes patches OSF415-410124 (371.00), OSF415-410173 (666.00) This patch corrects the following: • Fixes a problem that occurs when the default C compiler is used to compile a program using the following switches on the command line: c -compress -fast • Implements a new cc switch to allow the passing of the ld "-input file" switch to the linker via cc, without changing its relative position in the ld command line. The current method for doing this (-Wl,-input,filename) changes the order in which such a file is presented to the linker, and can result in an invalid transfer address in an executable, resulting in a segmentation fault. • Fixes a problem in cc that causes it to set the incorrect optimization level when the user specifies the "-O -migrate" options.
Patch 676.00 OSF415-410192	**Patch:** Console Terminal Printing During Panic Correctly **State:** New. Supersedes patches OSF415-027 (227.00), OSF415-030 (274.00), OSF415-410191 (675.00), OSF415-031 (379.00) This patch corrects the following: • Under heavy load, MX5 systems can exhibit the following error: "Invalid Page Table Entry on Scatter Gather access" or an undetected data corruption. This patch will eliminate the error and a possibility of a data corruption. • Under conditions where device drivers use the DMA_CONTIG flag for dma address space allocation, the DIGITAL Personal Workstation can exhibit extreme system malfunction such as system hang, erroneous machine checks, and data corruption. • Fixes a problem for several platforms that don't print to the console terminal during a panic correctly. The particular platforms involved are AlphaStation 600, AlphaPC 164, AlphaServer 1000A 5/XXX, AlphaServer 1000 5/XXX, AXPvme 100 SBC, and DIGITAL Personal Workstation 433au, 500au, 600au. • Fixes a problem in which correctable memory errors are being logged to the system console as well as to the binary error log. • Fixes a problem that can cause bad pages to not be flagged during memory testing.
Patch 681.00 OSF415-410198	**Patch:** syslogd Correction, (SSRT0499U) **State:** Supersedes patches OSF415-410088 (208.00), OSF415-410119 (367.00), OSF415-410142 (390.00) This patch corrects the following: • Fixes a problem in which the syslogd program cannot properly forward large messages to remote systems. It will either write them to the wrong facility (specified in /etc/syslog.conf) or write incomplete data. • Fixes a problem in which the syslogd daemon may hang when writing to a named pipe log file. • Fixes a problem in which syslogd will core dump if /etc/syslog.auth file has greater than 23 lines.

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

Patch 684.00 OSF415-410205	**Patch:** ddr_config Corrections **State:** Supersedes patch OSF415-410098 (270.00) This patch corrects the following: • Enhancement to the Ethernet driver for the DE500-XA Fast Ethernet Interface. This patch improves the failover time in an ASE environment when the cluster members use DE500-XA interfaces. • Fixes the following problems that may occur on some DE500 adapters: – The hardware setup operation may interrupt a pending ARP packet transmission. – If the cable to the adapter is not connected, the hardware setup operation will not execute.

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

Patch 689.00 OSF415-044	**Patch:** Various Kernel Fixes (SSRT0482U, SSRT0521U) **State:** New. Supersedes patches OSF415-410039 (5.00), OSF415-410034 (2.00), OSF415-400100 (48.00), OSF415-405036 (31.00), OSF415-400141 (63.00), OSF415-400165 (76.00), OSF415-410052 (13.00), OSF415-410059 (18.00), OSF415-405054 (38.00), OSF415-410062 (19.00), OSF415-405044 (35.00), OSF415-405053 (37.00), OSF415-405059 (39.00), OSF415-410049 (12.00), OSF415-400186 (89.00), OSF415-400201 (99.00), OSF415-400127 (57.00), OSF415-400197 (97.00), OSF415-410068 (22.00), OSF415-405062 (40.00), OSF415-400208 (103.00), OSF415-400198 (98.00), OSF415-400216 (109.00), OSF415-400221 (113.00), OSF415-400232 (121.00), OSF415-400233 (122.00), OSF415-400235 (146.00), OSF415-400242 (151.00), OSF415-405058 (166.00), OSF415-400250 (155.00), OSF415-400250-1 (155.01), OSF415-410070 (191.00), OSF415-400130 (58.00), OSF415-410074 (192.00), OSF415-410085 (197.00), OSF415-410087 (207.00), OSF415-400245 (153.00), OSF415-400266 (174.00), OSF415-400240 (149.00), OSF415-400289 (183.00), OSF415-400296 (187.00), OSF415-400298 (188.00), OSF415-400351 (224.00), OSF415-405098 (214.00), OSF415-400281 (229.00), OSF415-400283 (232.00), OSF415-400346 (243.00), OSF415-400353 (245.00), OSF415-400354 (246.00), OSF415-400367 (253.00), OSF415-021 (215.00), OSF415-400369 (255.00), OSF415-400373 (279.00), OSF415-400378 (280.00), OSF415-400284 (180.00), OSF415-400DIGITAL (281.00), OSF415-400401 (282.00), OSF415-400407 (278.00), OSF415-410102 (272.00), OSF415-410113 (296.00), OSF415-023 (217.00), OSF415-400356 (247.00), OSF415-400384 (283.00), OSF415-405123 (293.00), OSF415-410112 (295.00), OSF415-029 (228.00), OSF415-400414 (311.00), OSF415-400418 (314.00), OSF415-400420 (315.00), OSF415-400421 (316.00), OSF415-400441 (328.00), OSF415-400442 (329.00), OSF415-400451 (334.00), OSF415-400456 (336.00), OSF415-400461 (338.00), OSF415-400466 (341.00), OSF415-400469 (344.00), OSF415-405133 (359.00), OSF415-405134 (360.00), OSF415-405136 (362.00), OSF415-405145 (363.00), OSF415-410135 (376.00), OSF415-410122 (369.00), OSF415-410130 (375.00), OSF415-034 (381.00), OSF415-035 (382.00), OSF415-036 (383.00), OSF415-405153 (487.00), OSF415-405155 (497.00), OSF415-405162 (411.00), OSF415-405177 (425.00), OSF415-405185 (431.00), OSF415-405198 (438.00), OSF415-405199 (439.00), OSF415-405200 (440.00), OSF415-405206 (444.00), OSF415-405207 (445.00), OSF415-405209 (447.00), OSF415-405210 (448.00), OSF415-405221 (457.00), OSF415-405238 (469.00), OSF415-405243 (474.00), OSF415-405281 (479.00), OSF415-405292 (480.00), OSF415-410145 (391.00), OSF415-410155 (395.00), OSF415-410157 (399.00), OSF415-410158 (400.00), OSF415-405176 (424.00), OSF415-405229 (462.00), OSF415-032 (380.00), OSF415-037 (384.00), OSF415-410156A (396.00), OSF415-039 (688.00), OSF415-048 (692.00), OSF415-405189 (511.00), OSF415-405259 (519.00), OSF415-405268 (524.00), OSF415-405269 (525.00), OSF415-405276 (529.00), OSF415-405277 (530.00), OSF415-405278 (531.00), OSF415-405287 (537.00), OSF415-405289 (538.00), OSF415-405293 (540.00), OSF415-405299 (544.00), OSF415-405302 (547.00), OSF415-405305 (548.00), OSF415-405307 (549.00), OSF415-405325 (560.00), OSF415-405328B (705.00), OSF415-405330 (564.00), OSF415-405335 (567.00), OSF415-405340 (571.00), OSF415-405345 (575.00), OSF415-405348 (577.00), OSF415-405352 (579.00), OSF415-405355 (581.00), OSF415-405356 (582.00), OSF415-405357 (583.00), OSF415-405362 (587.00),

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

Patch 689.00 continued	OSF415-405363 (588.00), OSF415-405364 (589.00), OSF415-405366 (591.00), OSF415-405368 (592.00), OSF415-405371 (595.00), OSF415-405378 (601.00), OSF415-405383 (605.00), OSF415-405384 (606.00), OSF415-405392 (612.00), OSF415-405394 (613.00), OSF415-405DIGITAL (615.00), OSF415-405404 (619.00), OSF415-405416 (626.00), OSF415-405426 (629.00), OSF415-405429 (631.00), OSF415-405430 (632.00), OSF415-405431 (633.00), OSF415-405434 (636.00), OSF415-405443 (642.00), OSF415-405448 (646.00), OSF415-405450 (648.00), OSF415-410159 (659.00), OSF415-410164 (660.00), OSF415-410167 (662.00), OSF415-410170 (664.00), OSF415-410176 (668.00), OSF415-410178 (669.00), OSF415-410182 (671.00), OSF415-410187 (672.00), OSF415-410189 (674.00), OSF415-410193 (677.00), OSF415-410194 (678.00), OSF415-410195 (679.00), OSF415-410196 (680.00), OSF415-410203 (683.00), OSF415-410206 (685.00), OSF415-410208 (686.00), OSF415-410213 (687.00), OSF415-405190 (512.00) This patch corrects the following: • Fixes a problem in which network applications communicating to on of the host's own addresses, may hang, or receive the error message: no buffer space available The problem occurs due to a queue full condition on the interface. • This patch provides support for the fuser utility. This utility displays a list of processes that are holding references to a file on the file system that cannot be unmounted. • Fixes a problem in which the the lastcomm accounting command doesn't print the "S" flag at appropriate times. This patch also improves the performance of lastcomm. • Fixes a problem with the fsck command. When fsck is run on a non-existent file system or on a currently mounted file system, it returns a success status of zero. It should return a non-zero status. • This patch resolves a TCP/IP network hang due to IP Q ACK deadlock. When this condition occurs the IP Q becomes full due to saturation. Representative console messages indicating this condition are shown below: SIS00-00-root: IP q full, 315617 packets dropped in the last 5 mins. • Fixes a performance problem that occurs with UFS file systems. • Fixes a problem in which the ufs property list can become corrupted. • Fixes a problem with the exec() system function. A shell script that has "#! " as the first line of the script, invokes the program but does not set the effective user id for the execution of the program.

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

Patch 689.00 continued	• Fixes a number of problems relating to signals and POSIX 1003.1b timers in multithreaded programs running on multiprocessor systems. These problems can result in missed timer-expiration signals and system crashes. • Fixes a problem that occurs when the system panics with the following error message: kernel memory fault • The kernel panics with a "kernel memory fault", typically in either the vm_pg_alloc() or vm_zeroed_pg_alloc() routines. • This network patch, which greatly improves DIGITAL UNIX networking performance, is targeted at high traffic Web server systems or any system which handles a large number of TCP connections simultaneously; e.g., more than several thousand at one time. • This patch resolves a kernel memory fault. This patch is MANDATORY. • System panics with message "vm_map_swapout: negative resident count". • Fixes a kernel memory fault in ether_output packet filter, when running tcpdump. • Fixes a problem that occurs on all systems that use networking system. • Fixes ICMP REDIRECTS. When an ICMP REDIRECT is received, the routing table was updated properly, but the IP layer didn't use then new route information. • Fixes a problem in which the system can panic with "lock already owned by thread". • This patch is a kernel fix for network sockets left in FIN_WAIT_1 state forever. This patch contains a "tunable" kernel parameter. It is recommended that only experienced system administrators attempt to set this parameter from the default value. • The user or system UAC_NOPRINT settings are ignored when an unaligned access trap on a user address was taken while in kernel mode; the unwanted error message is still printed. • NetWorker Version4.2c requires this patch for new fcntl functionality. This layered product will not run desirably without this patch. • This patch allows tuneablity for existing two level task swapping scheme. • The ObjectStore application from Object Design, Inc. fails with the following error: "Fatal error Invalid argument(errno = 22) munmap failed: cl_mmap:" • Fixes a system crash when setting the date on SMP systems. • Devices sometimes cannot be accessed by the system after getting selection timeouts. • Fixes a network socket problem with select() missing state changes on clients from non-write to writable.

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

Patch 689.00 continued	• This patch allows tuneablity for existing two level task swapping scheme. • The ObjectStore application from Object Design, Inc. fails with the following error: "Fatal error Invalid argument(errno = 22) munmap failed: cl_mmap:" • Fixes a system crash when setting the date on SMP systems. • Devices sometimes cannot be accessed by the system after getting selection timeouts. • Fixes a network socket problem with select() missing state changes on clients from non-write to writable. • Fixes some hangs that can occur during the "syncing disks..." portion of panic processing, improves the reliability of getting a dump after a system panic, and also makes it more likely that AdvFS buffers will be synced to disk after a system panic. • The vmstat(1) command displays negative numbers when used with the '-P' option. Problem may not appear on all platorms or configurations. It is dependent on how the system constructs various internal data structures. • Prevents a "kernel memory fault" in bread() during sync operations. • Fixes "kernel memory fault" panics from the kernel malloc() routine, and threads hanging in vfs_busy() when file-on-file mounting (kernel option FFM_FS) is used with fattach()/fdetach() or System V STREAMS. • Fixes a problem that prevents an "options DCEDFS" line from being added to the kernel configuration file. Without the fix, the kernel build will fail with the error "ld: dcedfs.mod: setjmp: multiply defined". • Fixes a panic which occurs when a UNIX domain socket lock is being held while calling vrele(). • An enhanced fix to the solockpair() routine. This fix was needed because the routine was freeing a socket lock structure that was concurrently spun upon in lock_write(). Typical problem symptoms include kernel memory faults with sockets, mbufs and mblocks as well as hangs. Applications using sockets in a multithreaded, multicpu environment can experience a number of lock violations with the socket structures. This patch is MANDATORY to install on all systems. It will be effective on Uniprocessor systems when lockmode debugging is invoked. • Corrects a problem with an NFS V3 mounted AdvFS file system where under heavy I/O load, data being written to a file may be lost. Additionally, because file stats are not being saved, the file modification time may revert to a previous value. • Fixes a panic that prints "kernel memory fault". • Fixes a 'recursion count overflow' problem that occurs on DIGITAL UNIX systems. • Allows some third-party NFS v2 clients to experience a performance improvements. • This patch greatly reduces the number of "NFS stale file handle" messages logged to an NFS server system console.

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

Patch 689.00 continued	• Fixes a problem with the "ifconfig -a" command. At times, the command will not display all of the network interfaces. • Fixes a problem that causes systems to panic with a "kernel memory fault" from u_dev_lockop(). This has happened when a database tried to memory map a file. • Fixes the problem of audit_tool terminating prematurely the reading of a complete large log file via zcat. This usually occurs under gui control. • This is a mandatory patch for the following systems and conditions: – Systems that use program debuggers such as TotalView, Ladebug, dbx, or gdb – Systems that use the /proc file system in any other way (for example, the System V Environment ps command) – Systems that experience panics and hangs in the /proc file system – Systems that panic when running multithreaded programs that call an exec() function • This patch improves the performance of applications that map hundreds of thousands of files into the virtual address space. • This patch provides general support for Version A11 KZPSA firmware. • Fixes a problem in which a filesystem cannot be unmounted. The system displays a "Device busy" error message. • Fixes a problem that occurs when starting up a system that is running the auditing subsystem and the performance manager. The system panics with the following error message: kernel memory fault • Fixes a problem in which the kernel can panic with a "kernel memory fault" when attempting to push a signal state onto the stack of a thread in a multithreaded program.

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

Patch 689.00 continued	• Back-port of PTMIN-style multi-option kmem_debug settings. Changed all-or-one kmem_debug bucket selection to all-or-as-selected. Added two new kmem_debug options, KMEM_DEBUG_LINKS and KMEM_DEBUG_PROTECT. • Resolves an inode locking problem in the UFS iupdat() and itimes() functions. • This is a mandatory patch for SMP systems with AdvFS file systems. This patch fixes a performance degradation problem that may occur. • This patch is MANDATORY. This patch contains two vm fixes in both the the UFS and NFS code that collectively resolve a multitude of nfs and nfsd hangs. • This patch is in reference to BLITZ TD# 2278. Corrects a raw I/O data corruption problem that occurs when using database applications. The problem is seen when the new-wire-method is active. • Fixes a problem that may occur after a system panics. The system may hang when trying to do a crash dump. • Fixes a problem in which a system may crash if multiple bad blocks on a SCSI device are encountered simultaneously. • Fixes a problem where conversion from double-precision floating point numbers to single-precision floating point numbers may not round properly in IEEE mode when the result should be the smallest denormal. • Provides additional event logging by the SCSI/CAM disk driver to the binary.errlog file. • After a disk error occurs, mirror set switching may not happen soon enough to ensure high availability, or in some cases may not happen at all. • When a zero length message is sent to an invalid SVIPC message queue, kernel memory is corrupted. • Fixes a UFS file system problem. The system may panic with the following error message: panic spec_badop called • Eliminates the display of "Stack overflow: pid..." messages that may occur when running Ladebug. • Fixes a potential memory leak problem that occurs when using the KMEM_DEBUG_PROTECT option of the kmem_debug tuneable attribute. • This is a mandatory patch. This patch fixes a problem that occurs on programs that are linked with the pthreads library. After a parent process forks a child process, the child's floating point state may become corrupt. • Fixes a problem in which the uswitch system call does not work when an application tries to reset the USW_NULLP option.

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

Patch 689.00 continued	• Fixes a problem with the nfsd daemon. Although the maximum number of threads that nfsd can run is 128, the nfsd daemon will not start when the sum of UDP threads and TCP threads equals 128. • 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. DIGITAL has corrected this potential vulnerability. • Fixes a problem that occurs on AlphaServer 4100 systems. If no devices are attached to the KZPSA disk controller, the system may panic when attempting to perform I/O. • Fixes an AdvFS problem in which the system may panic with the following error message: thread_block: simple lock owned • Provides two new procfs ioctls (PIOCUSAGE and PIOCTUSAGE) to collect task and thread wait time statistics. • Fixes a problem that causes the system to panic with the following error message: u_anon_free: page busy • Provides a bugfix to avoid a panic that might result when running a mixed filesystem behind the HSZ70 Raid controller on the KZPSA-BB Fast10 Wide Differential adapter in cluster environments under DIGITAL UNIX V4.0C, in conjunction with Version A11 KZPSA firmware or greater. • Fixes two kernel memory faults in networking code. • Fixes a panic with the following error message: trap: invalid memory write access from kernel mode • Fixes a hang of an ASE AGENT and problems with the error recovery of the HSZ family of storage arrays. • Fixes a problem in which the host crashes when a user tries to delete a logical unit using hszterm. The following error message can be displayed: trap: invalid memory read access from kernel mode • Fixes a race condition whereby the pid_block() system call doesn not properly synchronize with signals. This problem could cause the system call to block and not take a signal when it is supposed to. • Fixes a data corruption problem that occurs on systems using Prestoserve. The problem may cause system panics. For example, an AdvFS system may panic with: "bad v1 frag free list" A UFS file system may panic with: "ialloc: dup alloc" • Fixes a read/write problem for buffers larger than 4GB. The read/write request would truncate to a maximum of 4GB, but return success, causing data corruption.

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

Patch 689.00 continued	• Fixes a problem in which the system may panic with the following message: simple_lock: lock already owned by cpu • Improves performance on low-memory (32MB) systems. • Fixes a problem with the ufs_fsck program in which filesystem corruption may occur on a running system when the root filesystem is mounted writable. • Corrects a problem where the NXM_IEEE_STATE_COPYIN/OUT macros need to save/restore the pcb nofault state. This was not happening. • Corrects a synchronization problem by blocking out hardclock before touching the state visible to the clock interrupt routine. • Corrects a problem in how the ps command reports its accumulated CPU time of all exited threads. • Fixes a problem where the umount of a filesystem will fail with "mount device busy", but no processes are accessing files in the filesystem. • Fixes a kernel memory fault panic in purge_fs_locks. This problem is normally only seen on ASE or TruCluster systems. • Extend the KMEM_DEBUG_PROTECT option of kmem_debug to the 8192-byte bucket. • Fixes a problem that occurs when KZPSA and KZTSA hardware resources needed to do I/O are unavailable causing a large number of events to be logged. The system can become sluggish and sometimes crash. This problem is seen on 8400 and 4100 systems with limited hardware scatter-gather memory resources. • Prevents a "kernel memory fault" in the bread() routine while performing sync operations. • Fixes a kernel memory fault in the networking code. • Fixed several problems with vfs file locking that could cause a crash including the file lock adjust logic, delete sleep lock logic, dead file lock logic, check/change granted logic, and insert file lock logic.

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

Patch 689.00 continued	• Fixes a problem that produces a core dump when running the quotacheck -a command. The following panic string is displayed: Segmentation fault at strcmp • 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. DIGITAL has corrected this potential vulnerability. • Fixes a "mount device busy" problem that occurs when a user cannot overwrite the file "core". This prevents the filesystem from being umount'ed. • Corrects a problem whereby large SMP configurations (greater than 8 CPUs) running DIGITAL UNIX will appear to have problem keeping their time synchronized. The symptoms usually show up while running a time synch protocol, such as NTP. Also, systems with 12 or 14 CPUs may experience performance slowdowns. • Improves performance on low-memory (32MB) systems. • Fixes a panic in the virtual memory management system. The system displays the following error message: trap: invalid memory read access from kernel mode • Fixes a kernel memory fault panic. This patch is mandatory for all multiprocessor machines. The system will crash with the panic string "Kernel Memory Fault". • Fixes a rounding problem in the kernel software completion trap handler that slightly reduces the IEEE denormalized multiply and divide accuracy. It has no effect on typical arithmetic operations. • Fixes an AdvFS response time problem that occurred when an application with many random access reads of many files was being slowed down by the resulting number of writes to disk. • Fixes a problem where during tape operations, the SPACE commands can not be interrupted. • Fixes a problem in which a system panics with a "kernel memory fault" error message. The problem occurs when a tape drive is plugged into the slot previously occupied by a disk. • Corrects a problem where the code around referencing a tape device pointer is not synchronized and a kernel memory fault results. • Under certain conditions, the message "ctape_strategy: READ case and density info not valid." was being printed for every read from tape. This change will print the message only once.

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

Patch 689.00 continued	• Corrects a problem in memory allocation where a tasks resident count could become inconsistent, causing a panic. • Fixes the following problems: – Process hangs caused by file references on raw devices accesses not being held. – A "kernel memory fault" system panic caused by AIO not cleaning up test headers when processes exit. • Fixes a problem with the vmstat -M command. vmstat -M shows an invalid byte count associated with the FREE malloc type. • Corrects a problem where a flag, TF_PSUSP, was not being cleared. • Fixes a problem that produced a deadlock betweeen process threads. Typically, the deadlock caused the msfs_getpage routine to wait forever for a lock to be released. • Corrects a problem that causes a "pmap_ssm_destroy: wired pages" crash. • Corrects a performace problem with POSIX timers. • Fixes a problem where the system will panic with "kernel memory fault". • 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. DIGITAL has corrected this potential vulnerability. • Fixes a networking problem that occurs when the kernel variable ipport_userreserved is set to 65535. • In some instances, a message size of zero passed to msgsnd() can result in a kernel memory fault panic. • Prevents a system panic from m_copym(). • Fixes a problem in which a a cluster member panics, when the Production Server or Available Server software attempts to relocate a tape service. • Avoids a "kernel memory fault" panic from sigsgdisp(). The problem has only been seen when shutting down an Oracle database. • Fixes a problem with memory being wasted by Mach IPC kernel message routines because they were assigned fixed sizes of memory (large or small, depending on the routine). Now, the memory allocation for the IPC routines has been changed to allocate only the memory each routine requires. • Fixes a problem within LMF. The LMF user license list (OSF-BASE or OSF-USR) was not being decremented when a logout occurred. This occurs on systems with C2 security enabled and the system setup as a DCE Security server. • Corrects a small accounting problem where the measured time for a process was an integral rather than mean value. • Corrects a problem that would randomly cause kloadsrv(8) to crash and improperly load/unload modules.

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

Patch 689.00 continued	• Fixes a problem in which a failed KZPSA adapter panics the kernel. It also fixes a problem in which CAM status was returning an incorrect "NO HBA" status for miscellaneous SIMPORT errors, instead of the correct "CAM BUSY" status. • Changes the sbcompress_threshold type to unsigned from signed since you could not set the sysconfig value for this flag correctly. • Fixes a problem that caused the system to panic with the string "kernel memory fault". • Fixes a problem in which the system can panic with "lock already owned by thread" or "kernel memory fault". • 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. DIGITAL has corrected this potential vulnerability. • Fixes a TCP/IP performance problem in the tcp_reass() function. • Removes extraneous debug code. • Fixes a system panic "rtfree 2" on multi-cpu systems. • Fixes a problem with the "vmstat -M" command. This command displays negative values for memory usage by type and AdvFS buffer usage. • - Fixes a problem in which a recursive panic occurs during certain lockmode violations. • Fixes the bufpages calculation so that it takes granularity hints into account. • Fixes a problem that can cause asynchronous I/O to fail. • Fixes a problem that was caused by both floating point and integer overflow exceptions setting the si_code member in the siginfo structure to FPE_FLTOVF. • Fixes a problem with NFS conversion of a file's vnode number to a file handle number. The file id was truncated improperly, generating EOVERFLOW errors. • Fixes a problem in which savecore incorrectly reports a negative number of dumped bytes. This problem may be seen when doing a full crash dump on a system that has more then 2 gigabytes of memory. • Corrects a potential boot panic problem by limiting the size of the bufcache. • Fixes the following two problems that occur on an NFS file server using a Network Appliance server: – New files may not be listed in directory reads. For example, when the ls command is used not all the files may be listed. – When a directory listing is requested from a Network Appliance server, more data than was requested may be returned and the extra data is lost by the DIGITAL UNIX client. The problem can be seen by doing using the ls command; not all the files on the server are listed. • Fixes a virtual memory problem in which an uninitialized pointer in u_dev_protect() causes a kernel memory fault to occur. • Fixes a virtual memory problem that may cause a system to panic with one of the following messages: "pmap_begin_mutex_region timeout" or "simple_lock timeout".

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

Patch 689.00 continued	• Fixes a problem in the kernel that caused dynamically loaded PCI/ISA drivers to crash the system with the following panic: kernel memory fault • Resolves systems from hanging during boot. Disabling CRD interrupts during boot caused PAL to NOT deliver the interrupt to the OS and therefore NOT clear the error, so a infinite recursion interrupt hang results. This patch is MANDATORY for all hardware platforms. • Fixes a problem in which the sysconfig command produces an error when a subsystem name of 15 characters is used. The following error message is displayed: framework error : copying memory to / from kernel • Corrects an NFS client problem that results in a kernel memory fault system panic. • Fixes various problems caused when a set UID/GID program dumped core. The problems included system panics and "mount device busy" errors when trying to umount the filesystem. • Corrects a problem that can result in a kernel memory fault during heavy SCSI I/O, particularly on a small-memory system. • Fixes the following problems in AdvFS: – A operating system hang condition. The hang condition exists due to processes deadlocking in the AdvFS code. – AdvFS does not return an error when a user opens a file in O_SYNC mode and power is lost on the disk drive. – A locking error in the AdvFS fs_write() routine. • Fixes a problem with the KZPSA and KZTSA SCSI adapters. The adapters will hang if the SCSI cable is disconnected from them. • Fixes a problem when a setuid program is exec'ed, and the error message "privileges disabled because of outstanding IPC access to task" is issued. • Fixes a kernel memory fault in cansignal(). • Fixes a problem that occurs on AdvFS systems. The system will panic with the following error message: malloc_overflow: guard space corruption • Fixes the problem in which a DIGITAL UNIX system can randomly panic when more than 255 network interfaces are configured. • Fixes a problem when a processor is commanded to stop during a heavy load but does not actually halt. • Corrects a problem seen with DECthreads tests that use fork(2). • Corrects a potential problem in the handling of a ieee_get_state_at_signal(3) C-library call. • Fixes a problem that occurs with applications based on POSIX message queues. During certain high activity periods, processes may hang when trying to access the message queue. • Corrects a simple lock timeout problem in several vm_page routines.

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

Patch 689.00 continued	• Fixes two Kernel Memory Faults in DIGITAL UNIX Path MTU discovery code. • Prevents a kernel malloc leak when changing the protection of a System V shared memory region that uses gh-chunks. • Fixes a problem with the CPU auto_action console environment variable. If the auto_action console environment variable is set to BOOT or RESTART, when the CPU is to be stopped, the processor immediately boots and the user can not observe that the CPU had halted. • Fixes a problem in the AdvFS logging code, The way locking was implemented was causing degraded performance. • Fixes a problem with the vmstat -P command, which was incorrectly formatting output. • Fixes a system panic caused by a multithreaded process with profiling turned on. The system panics with the following message: "lock_terminate: lock held" • Fixes a problem with user stack pointers not being saved properly in kernel crash dumps for running threads. • 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. DIGITAL has corrected this potential vulnerability. • Fixes a problem with the way the ps utility collected CPU usage information. One effect of the problem was that processes run with nice values of 18 or greater had contention problems based on the incorrect CPU values. • Fixes a problem whereby the contiguous memory allocator uses physmem to calculate percentage of memory to reserve. On a system with memory holes, this results in reserving non-existent pages for contiguous memory. • Fixes an ASE NFS problem that occurs on ASE systems with KZPBA disk controllers. The system crashes with a "simple_lock timeout" panic.
Patch 690.00 OSF415-045	**Patch:** Compiler Causing CPU Exception Errors **State:** New Fixes a compiler problem that was causing CPU EXCEPTION errors to be generated in the system binary error log. The problem was experienced during bootstrap on 2100A cpus.

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

Patch 693.00 OSF415-400437A	**Patch:** AdvFS Consolidated Patch **State:** New. Supersedes patches OSF415-410031 (1.00), OSF415-400105 (49.00), OSF415-400148 (67.00), OSF415-400125 (55.00), OSF415-400176 (85.00), OSF415-400176-1 (85.01), OSF415-400217 (110.00), OSF415-400228 (118.00), OSF415-400239B (164.00), OSF415-400231 (120.00), OSF415-400231-1 (120.01), OSF415-400259 (161.00), OSF415-405094 (213.00), OSF415-400315 (203.00), OSF415-400342 (240.00), OSF415-400344 (242.00), OSF415-405107 (266.00), OSF415-405112 (267.00), OSF415-410092 (268.00), OSF415-405120 (276.00), OSF415-400389 (305.00), OSF415-400445 (331.00), OSF415-400449 (333.00), OSF415-400476 (346.00), OSF415-400482 (348.00), OSF415-400489 (350.00), OSF415-405146 (364.00), OSF415-410118 (366.00), OSF415-410123 (370.00), OSF415-410128 (373.00), OSF415-410129 (374.00), OSF415-400497 (385.00), OSF415-405241 (386.00), OSF415-410129-1 (374.01), OSF415-405148 (403.00), OSF415-405156 (406.00), OSF415-405170 (419.00), OSF415-405171 (420.00), OSF415-405172 (421.00), OSF415-405205 (443.00), OSF415-405214 (451.00), OSF415-405215 (452.00), OSF415-405219 (455.00), OSF415-405226 (459.00), OSF415-405228 (461.00), OSF415-405231 (463.00), OSF415-405232 (464.00), OSF415-405235 (467.00), OSF415-405239 (470.00), OSF415-405242 (473.00), OSF415-405253 (478.00), OSF415-405240 (471.00), OSF415-410163 (402.00), OSF415-410126 (387.00), OSF415-410156B (397.00), OSF415-405249 (515.00), OSF415-405251 (516.00), OSF415-405275 (528.00), OSF415-405280 (533.00), OSF415-405283 (534.00), OSF415-405284 (535.00), OSF415-405298 (543.00), OSF415-405310 (551.00), OSF415-405323 (559.00), OSF415-405334 (566.00), OSF415-405344 (574.00), OSF415-405385 (607.00), OSF415-405398 (616.00), OSF415-405400 (617.00), OSF415-405427 (630.00), OSF415-405434 (636.00), OSF415-405437 (638.00), OSF415-405438 (639.00), OSF415-405444 (643.00), OSF415-405467 (652.00), OSF415-410159 (659.00), OSF415-405203 (442.00) OSF415-410169A (663.00), OSF415-410180 (670.00), OSF415-410202 (682.00), OSF415-405286 (536.00) This patch corrects the following: • An AdvFS data corruption problem can occur in user files. This problem will not produce either a core file or return non-zero system codes when accessing the corrupted file. • The verify command does not detect corrupted files. • Multithreaded applications that call the pthread_mutex_destroy routine may fail when there are no threads referencing the mutex. This is caused by a race condition inside the pthread_mutex_unlock code. The typical symptom will be a return value of EBUSY from pthread_mutex_destroy. • Fixes a problem with AdvFS in which the following two panics occur: AdvFS Exception Module = 1, line = 1891 kernel memory fault • Systems running with AdvFS and LSM under heavy I/O loads can have sluggish interactive performance. In a DECsafe environment, these systems can encounter unexpected relocation of services. • Idle time is reset on broadcast message when AdvFS is the root file system.

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

Patch 693.00 continued	• Fixes an AdvFS hang that could occur while running vdump. • Fixes a problem where AdvFS hangs in routine cleanup_closed_list. • Fixes a system panic with the message "simple_lock: time limit exceeded". • Fixes an "ADVFS EXCEPTION, Module = 26" panic that occurs after an "advfs I/O error" console message. • Fixes a problem that occurs on AdvFS system. When a user exceeds the quota limits, an excessive number of user warning messages are sent to the system console if the terminal is inaccessible. • Fixes a problem where the vrestore program does not report failed exit status appropriately on incomplete or incorrect commands, corrupt or invalid saved sets, or file open failures. • Fixes a problem that occurs on systems running AdvFS. The system panics with the following error message: panic (cpu 0): bfs_invalidate: not on free list syncing disks...done • Fixes problems with the AdvFS filesystem commands "quotacheck -a" and "vquotacheck -a". These commands erroneously set all quotas for users to values derived from the last AdvFS fileset in /etc/fstab, rather than the correct values for each individual fileset. • Fixes a problem that occurs on AdvFS systems. The system will panic with an error message similar to the following: panic (cpu 0): kernel memory fault • Fixes a problem that occurs on SMP systems with an AdvFS filesystem in which the system panics with the following message: simple_lock: time limit exceeded • When a user attempted to restore a vdump, which had been done with the "-D" option and included directories for which Access Control Lists (ACL's) had been declared, the vrestore program was failing to restore ACL's on directory files and issued warning messages. When a user specified the "-t" option, vrestore erroneously attempted to restore proplists on files that had them; issuing warning messages. • Fixes a panic with the panic string "spec_badop called" that can sometimes occur when an fpathconf system call is issued for a file in a AdvFS filesystem. The panic has following stack trace: panic (s = "spec_badop called") spec_badop fpathconf syscall _Xsyscall • Fixes a problem in which a system hang or core dump occurs when on program inadvertently overwrites the contents of another program. • Fixes an AdvFS problem in which the "advfsstat -n" command causes a core dump. The system displays the following error message: Memory fault(coredump)

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

Patch 693.00 continued	• Fixes a problem that occurs on AdvFS systems. If the "ls -l M1" command is given in a .tags directory, the fileset will become unmountable. If the system is then halted, a panic will occur. • Fixes an AdvFS problem in which improper handling of I/O queues cause either a kernel memory fault or the following panics: Fixes an AdvFS problem in which improper handling of I/O queues cause either a kernel memory fault or the following panics: "bs_invalidate: cache rundown" "rm_or_moveq: ioDesc not on a queue" • Fixes a problem that occurs on an AdvFS file system. While the symptoms of these AdvFS problems vary, the most common is a panic with the following error message: bs_frag_alloc: pinpg faild\n N1 = -1035 Alternately, bs_frag_dealloc: pinpg faild\n N1 = -1035 • Fixes an AdvFS problem that causes the system to panic with the following error message: simple_lock: lock already owned by cpu • Fixes a system panic when shutting down to single user mode using one of the following commands: – # shutdown now – # init s when AdvFS is the root or usr filesystem. • Fixes a problem with the vrestore command. When restoring a multi-volume tape archive, if the tapes that follow the first tape are write-protected, the following error message is displayed: vrestore: can't open device file • Corrects problems with AdvFS performance regression, and two AdvFS race condition situations between multiple routines that can cause panics. • Adds features and corrections to the AdvFS verify utility. • Fixes the following problems on systems with the AdvFS filesystem: – The mcellCount on-disk was not being updated as files were being migrated and this resulted in a panic situation during defragment and migrate operations. – A race condition on can result in a system panic with the following error message: panic (cpu 0): bs_frag_alloc: pinpg faild – During defragment and migrate operations, a lock is not released which hangs the system next time a thread tries to obtain the lock. – When executing /sbin/advfs/verify command on an unmounted AdvFS domain, the system will panic with the following panic string: panic_string: 0xfffffc00006cad90 = "kernel memory fault"

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

Patch 693.00 continued	• Fixes a problem that occurs on an AdvFS file system. The system may panic with the following error message: ADVFS INTERNAL ERROR: dealloc_bits_page: can't clear a bit twice • Corrects a kernel read fault panic condition that occurs when the AdvFS verify utility runs. The panic message looks like: trap: invalid memory read access from kernel mode panic (cpu 0): kernel memory fault • Fixes a race condition that occurs on an AdvFS file system. The system panics with the following error message: panic (cpu 0): bs_frag_alloc: pinpg faild • Fixes a problem that occurs on an AdvFS file system. An AdvFS lock is not released which hangs the system next time a thread tries to obtain the lock. • Fixes an AdvFS problmem that causes a lockmode 4 system panic. • Fixes AdvFS performance problems. • Fixes a problem in which vrestore can cause an occasional core dump (Foating Exception). • Fixes a problem that occurs on AdvFS file systems. A kernel memory fault occurs on the AdvFS file system when accessing nfs-mounted files. • Provides a performance improvement for AdvFS system. • Corrects a situation where a quotacheck can cause a system panic. • A system using an AdvFS clone fileset can panic with either a kernel memory fault in bs_real_invalidate_pages(), or with the panic string: "bs_real_invalidate_pages: buf refd or pinned" • Corrects a panic and hang situation due to a limit of advfs access structures. • Fixes a problem caused by the vdump command. When a user entered Ctrl/C to terminate a vdump operation, the command returned an incorrect status and mistakenly updated the /etc/vdumpdates file. • Fixes an kernel memory fault panic. The system displays the following error message: trap: invalid memory read access from kernel mode • Corrects a problem where the mcellCount on-disk was not being updated as files were being migrated and this resulted in a panic situation. • Corrects a problem with domain panics that could possibly cause the system to panic. A new AdvFS error number (E_DOMAIN_PANIC) (-1028) was created. • Fixes a problem that occurs when the user attempts to fill an AdvFS: the system crashes and displays the following panic: lock_write: hierarchy violation

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

Patch 693.00 continued	• Fixes a problem caused by the vrestore command. The command would fail when restoring multiple savesets from a TZS20 tape drive. • Fixes a problem that occurred when an AdvFS panic crashed the customer's system but the visible symptom was a crash due to a kernel memory fault. • Fixes the following problems that occurs on AdvFS system: – Race conditions occur due to threads seeing out-of -date extent maps. – A previous patch applied as a workaround to other extent map changes cause the system to hang. Applying this patch fixes this problem. – This patch fixes a problem with in-memory extent map locking that occurs on AdvFS systems. The problem can cause panics due to kernel memory faults or simple lock timeouts. • Corrects a problem where the mcellCount on-disk was not being updated as files were being migrated and this resulted in a panic situation. • Fixes an AdvFS response time problem that occurred when an application with many random access reads of many files was being slowed down by the resulting number of writes to disk. • Prevents a "kernel memory fault" in the msfs_reclaim() routine on systems using AdvFS. • Fixes a problem with the chfsets command. When a root user exceeded the fileset quota (which root is allowed to do), the chfsets command reported negative values for the free and available blocks in the fileset. • Fixes a kernel memory fault problem that occurs on AdvFS file systems. The system displays the following error message: panic: kernel memory fault at spec_reclaim() • Fixes an AdvFS problem that occurs when unmounting a domain. An unmount thread was waiting on a variable to be set to zero before continuing, but the routine that was to set the variable to zero never did. • Fixes a problem that crashed the system while it was running a "collision" test. The process would hang on a lock, never be woken, and crash the system.

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

Patch 693.00 continued	• Fixes a problem with the vrestore command. The command had returned a success status code even though it had restored an incomplete file during the operation. • Fixes a problem with the AdvFS fs_write routine, which would mishandle partial writes after detecting an error. • • Corrects a problem where a panic would occur when running rmtrashcan on a clone. • Fixes a problem with AdvFS, which caused a system panic with the following messge: log_flush_sync: pingpg error The system panic occurred when the AdvFS domain had already issued a domain panic and a user application then attempted to close a file in that domain. • Fixes several problems with the vrestore command, all related to handling and parsing of terminal I/O: – Interactive shell's handling of space characters – Displaying of files containing non-printable characters to a terminal during interactive's ls command, -t, -v, or -l options – Interactive mode commands piped from stdin – Prompting and requesting of input from a terminal during ctrl-c signal handling • Fixes a problem in AdvFS that produced the following system panic: bs_logflush_start: cannot write lsn • Fixes a problem with messages in system logs that reported AdvFS user and group quota limits. The messages were unclear: the user could not determine from them which users or groups were reaching the quota limits. • Fixes several problems associated with AdvFS tag files and directories, including displays of erroneous data and system panics. • Fixes three verify command problems: – The command was displaying a large volume of meaningless data. – When it encountered a nonrecoverable error, the command did not properly exit. – The command sent some error messages to stderr, some to stdout. • Fixes a problem in AdvFS locking code which causes the following panic: kernel memory fault

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

Patch 693.00 continued	• Fixes a problem in AdvFS that was causing a memory leak. • Fixes the following problems in AdvFS: – A operating system hang condition. The hang condition exists due to processes deadlocking in the AdvFS code. – AdvFS does not return an error when a user opens a file in O_SYNC mode and power is lost on the disk drive. – A locking error in the AdvFS fs_write() routine. • Fixes a problem with AdvFS that caused a page fault and the following panic: panic (cpu 0): kernel memory fault • Fixes two AdvFS problems: – An error message was misleading when a DIGITAL UNIX Version 4 system attempted to access a file domain created by DIGITAL UNIX Version 5. – A state field in an AdvFS data structure was initialized, but not maintained. • Fixes a problem where a system hang can occur when creating an AdvFS file system, such as on "/ "or "/usr" partitions, on small memory systems (e.g., 32-64 mb). • Fixes a problem where user files or the AdvFS frag file could lose data, if they are updated during an AdvFS migration (that is, during a balance, defragment, migrate, or rmvol of their AdvFS domain). • Fixes a problem that occurs on AdvFS systems. The system will panic with the following error message: malloc_overflow: guard space corruption • Fixes a problem in the chvol command. chvol was not recognizing LSM volumes. • Fixes an AdvFS problem that occurs when the rmvol command is stopped before the commmand successfully removes a volume from a domain. As a result, the showfdmn and addvol commands interpreted the volume as still in the domain (although with no data available) and a balance operation returned the following AdvFS error message: get vol params error EBAD_VDI (-1030) • Fixes a problem in the AdvFS system. The log file corruption caused panics during recovery and failures displaying one of the following messages: ftx_fail: lgr_read failure or ftx_fail: dirty page not allowed • Fixes a problem in AdvFS, which causes a system panic when a truncate operation is performed on a file. The panic is: log half full • Fixes a problem in which the vquota, vedquota, quota, edquota, dump, csh, and nslookup commands will sometimes display incorrect error messages for non-English locales.

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

Patch 694.00 OSF415-405440B	**Patch:** Mutex Lock Problem in TLI **State:** Supersedes patches OSF415-400171 (82.00), OSF415-400196 (96.00), OSF415-400264 (173.00), OSF415-400151 (70.00), OSF415-400385 (308.00), OSF415-400405 (310.00), OSF415-400405B (490.00) This patch corrects the following: • Fixes a mutex lock problem in TLI. The problem causes multithreaded TLI applications to block forever. • Fixes the problem of t_optmgmt() T_NEGOTIATE calls returning T_SUCCESS, but not actually negotiating the socket options. This behavior is a UNIX95 specification standard compliance bug. • Fixes a problem that manifests itself by the system hanging or becoming inoperable when a number of XTI connections reaches 500. • Resolves a hang in the xticlose() routine and a kernel memory fault in the xti_discon_req() routine. • Corrects a problem with the xti/streams interface module which could result in a kernel memory fault panic during use by xti application programs. • Fixes a problem with the implementation of the TPI interface. This problem occurs if you are using DIGITAL's XTI libxti library with a third-party (non-DIGITAL) STREAMS driver. • Fixes libtli/libxti to correctly handle a continuation data message still on the stream head.
Patch 695.00 OSF415-405440C	**Patch:** Security (SSRT0296U) **State:** Supersedes patches OSF415-400331-1 (221.01), OSF415-400241 (219.00), OSF415-400189 (91.00), OSF415-999 (298.00), OSF415-405165C (416.00) This patch corrects the following: • This patch allows customers to create hashed passwd databases from large passwd files by using a new option (-s) to the mkpasswd command. The -s option increases the block size of the database page file. • This patch fixes a problem in which multithreaded applications that reference a pthread_mutex_destroy routine may fail with EBUSY or the application may hang. • A potential audit vulnerability has been discovered, where under certain circumstances, the audit trail of a user may be compromised. DIGITAL has corrected this potential vulnerability. • Fixes libtli/libxti to correctly handle a continuation data message still on the stream head.

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

Patch 696.00 OSF415-400437B	**Patch:** libc Corrections, Security (SSRT0425U, SSRT0296U) **State:** New. Supersedes patches OSF415-400080 (45.00), OSF415-400106 (50.00), OSF415-400119 (53.00), OSF415-400133 (60.00), OSF415-400139 (62.00), OSF415-400143 (64.00), OSF415-400153 (72.00), OSF415-400154 (73.00), OSF415-400189 (91.00), OSF415-400131 (59.00), OSF415-400195 (95.00), OSF415-400210 (104.00), OSF415-400226 (116.00), OSF415-400227 (117.00), OSF415-400239 (148.00), OSF415-400241B (150.00), OSF415-400241 (219.00), OSF415-400261 (163.00), OSF415-400302 (189.00), OSF415-400307 (220.00), OSF415-400331 (221.00), OSF415-400331-1 (221.01), OSF415-400323 (299.00), OSF415-400334 (237.00), OSF415-400348 (244.00), OSF415-400372 (257.00), OSF415-400400 (286.00), OSF415-400402 (284.00), OSF415-400348 (244.00), OSF415-400408 (287.00), OSF415-400410 (288.00), OSF415-400417 (313.00), OSF415-400430 (323.00), OSF415-400448 (332.00), OSF415-405168 (417.00), OSF415-405169 (418.00), OSF415-405181 (428.00), OSF415-405191 (434.00), OSF415-405217 (453.00), OSF415-400203-1 (100.01), OSF415-400115 (51.00), OSF415-405175 (423.00), OSF415-405165A (414.00), OSF415-410156C (398.00), OSF415-405272 (526.00), OSF415-405308 (550.00), OSF415-405312 (553.00), OSF415-405321 (558.00), OSF415-405341 (572.00), OSF415-405349 (578.00), OSF415-405380 (602.00), OSF415-405381 (603.00), OSF415-405391 (611.00), OSF415-405403 (618.00), OSF415-405520 (653.00), OSF415-410172 (665.00), OSF415-405317 (556.00) This patch corrects the following: • Fixes a problem with the DECthreads "legacy" library. Specifically this patch addresses the potential hang of programs that use the Draft 4 for pthread_once(). • Fixes a problem in which multithreaded applications that reference a pthread_mutex_destroy routine may fail with EBUSY or the application may hang. • Fixes a problem whereby mkpasswd fails for /etc/passwd files that are very large (containing roughly 30 thousand to 80 thousand entries). • Fixes problems that might cause threaded programs running under DIGITAL UNIX 4.0 to hang. Specifically, this patch addresses situations related to DECthread bugcheck, pthread_once() or cma_once(), and unhandled exceptions. • Fixes problems in threaded programs related to DECthreads bugchecks, fork(), stack corruptions and exception handling problems. This patch may also fix problems with non-threaded programs relating exception handling. • Fixes threaded applications seeing a deadlock with fork(), premature stack overflows, corrupted mutexes, and orphaned condition variable or mutex blocking structures. • Fixes problems in threaded applications with incorrect signal behavior and thread creation failures using user allocated stacks. • A potential security vulnerability has been discovered in BIND (Domain Name Service), where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability. • Fixes a problem in which mallopt(M_MXFAST), instead of making malloc() faster makes it as much as 65 times slower.

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

Patch 696.00 continued	• Fixes a problem where a call to popen() hangs after a bad call to pclose() in a threaded program. • 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. DIGITAL has corrected this potential vulnerability. • Fixes a problem that may cause older call_shared FORTRAN applications to find missing symbols in libc.so. • Fixes a deadlock problem that may occur with multithreaded applications calling any of the functions for getting system database information (gethostent, getservent, etc.) and which also call fork. The deadlock may occur when such applications are run on systems configured to use YP services. • Fixes a problem that occurs after a user logs into a system with an SRV4-style LAT device. When the ttyslot function is called, the system fails to find the device and returns a value of zero, indicating an error in the ttyslot function. • Fixes a problem that prevents gethostent() from returning all YP or bind served entries. • Fixes a problem in which the interaction of signals with setjmp/longjmp called repeatedly in a loop was causing a segmentation violation and core dump in a customer's application. • Fixes problems with redundant close operations on file descriptors by Network Information Services (NIS) and Remote Procedure Calls (RPC) in multithreaded applications. • Fixes a problem in which the rcmd function may cause the system to dump core. • This is a mandatory patch for DIGITAL UNIX 4.0. Fixes the following two problems that occur in the DECthreads core library: – The process blocked signal mask, as set by sigprocmask() is cleared in the child process following a fork(). – Under certain load conditions, a DECthreads bugcheck occurs in pthread_kill(). This results in a core dump. • Allows customers to create hashed passwd databases from large passwd files by using a new option (-s) to the mkpasswd command. The -s option increases the block size of the database page file. • Fixes a TCP/IP problem that can occur with programs linked with the libc library. These programs may return a value of (-1) when calling the svc_tcp() function. • Fixes a deadlock issue between fork() processing and exception handling on DIGITAL UNIX 4.0c. An exception occuring during a fork() operation would cause the child and parent processes to hang with no cpu activity. • Fixes a problem in libc. The allocation of pty's sometimes doesn't work correctly. This can cause problems with the EMACS editor. • Fixes two problems in the DECthreads library: – On multiprocessor platforms, condition variable broadcasts were occassionally being lost. – Stack unwinding during exception processing was losing contexts, resulting in incorrect stack traces. • Corrects a problem related to the statically initialized mutexes in DECthreads library (libpthread.so).

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

Patch 696.00 continued	• Fixes a problem whereby a call to the libc dbm_open() routine followed immediately by a call to dbm_close() causes hashed database directory files to be truncated. • Corrects a problem which occurs when pthread_cond_timedwait() is called with a large timeout value (greater than 23 days). • Fixes a problem with call_shared executables that are linked with libc.a instead of libc.so. A symptom of this problem is that routines like dlopen(3) and __fini_* routines are not run. • Fixes a problem that causes systems to panic with a "kernel memory fault" from u_dev_lockop(). This has happened when a database tried to memory map a file. • There is a problem in the Bind 4.9.3 patch which may cause incorrect messages to be reported. It may also cause statically linked programs using certain network functions in libc to core dump. • Fixes a problem with the auditd daemon. If auditd is logging to a server and the server becomes unavailable, the CPU usage for the daemon rises dramatically. • Fixes a problem in which RPC client functions do not correctly handle system calls interrupted by a signal (EINTR errors). • Fixes a problem that causes the readdir_r() function to read past the end of its input buffer. • A potential audit vulnerability has been discovered, where under certain circumstances, the audit trail of a user may be compromised. DIGITAL has corrected this potential vulnerability. • Fixes a DECthreads problem in which a threaded program may unexpectedly abort a process. • Fixes a bug found in 'pthread_kill' call. The bug may cause a thread program to terminate when the program tries to send a kill signal to a terminated thread. • Fixes a problem whereby exceptions propagating out of (or thrown from) __init routines in C (or C++) programs are not caught by the last chance handler and result in an infinite loop. • Fixes a problem with the syslog function. Some syslog messages may fail to get written to a log file when the system is experiencing a heavy I/O load. • Fixes a problem with rexec(3) losing socket descriptors. • Fixes a problem with the statvfs function. statvfs returns a wrong status when the file system is full. • Fixes a problem which occurs when a program attempts to create a thread with stacksize or guardsize greater than maximum signed long integer. • Corrects two problems: – A process hang when an application linked with libpthread performs a realloc(0,0). – A memory leak when small blocks are allocated with valloc(). • Fixes a problem in the DECthreads library for DIGITAL UNIX. During a fork() operation, DECthreads temporarily replaces its signal-to-exception mapping for synchronous signals by installing the system default handler. This fix permits any user-installed handlers to remain in place during the fork() operation.

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

Patch 696.00 continued	• Fixes an AdvFS response time problem that occurred when an application with many random access reads of many files was being slowed down by the resulting number of writes to disk. • Fixes a scanset processing problem in swscanf(). • Fixes a problem that causes a segmentation fault when doprnt calls strlen with non-null-terminated char arrays. • Fixes a problem with disklabel, where the command failed if the device was unable to provide disk geometry information. • A call to dbm_open() followed immediately by a call to dbm_close() caused hashed database directory files to be unnecessarily flushed. The ndbm routines were not threadsafe because of the definition and use of buffer ovfbuf, and dbm_open had some problems in its error handling code. The calculation of the page block size in dbm_open() did not make some necessary checks on size limits. • Fixes a problem in the audit daemon when it is used as a network server. Child auditd processes that are serving network connections fail to reap their child processes (such as when log files are compressed), leaving them as defunct processes on the system. • Resolves a problem with Enhanced Security not handling a voucher correctly from some other security mechanism such as DCE. The scenario to reproduce the problem would be: a user incorrectly enters his username at the first "login:" prompt, but subsequently corrects the login name when prompted again after the first failure. Without this patch, the user upon successfully typing their login/password on the second try would still receive the message "login incorrect". • Fixes a problem with printing floating point values using the width and precision specifiers. Previously, the leading and trailing zero counts were often miscalculated. • Fixes a memory leak in the libc glob() function. • Fixes a virtual memory problem that may cause the system to panic with one of the following messages: pmap_begin_mutex_region timeout or simple_lock timeout • 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. DIGITAL has corrected this potential vulnerability. • Fixes a problem in which BIND client applications are not able to resolve node names. Network applications running on a BIND client such as ping, telnet, and ftp using node names that are resolved by a BIND server will result in resolution errors such as "unknown host". • Adds automatic detection of a cdfs file system for the mount(8) command. • Fixes a problem in which the vquota, vedquota, quota, edquota, dump, csh, and nslookup commands will sometimes display incorrect error messages for non-English locales.

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

Patch 697.00 OSF415-405453B	**Patch:** libcurses Static Library Fix **State:** New Fixes a problem with the curses library. The infocmp command dumped core because two curses terminal capability tables were out of sync with each other.
Patch 698.00 OSF415X11-405011A	**Patch:** xterm Correction, Security (SSRT0422U, SSRT0547U) **State:** Supersedes patches OSF415X11-400010 (140.00), OSF415X11-400017 (201.00), OSF415X11-400021 (275.00) This patch corrects the following: • Fixes a problem in which the output of the "last" or "finger" command lists users that are not currently logged in. • 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. DIGITAL has corrected this potential vulnerability. • Fixes a memory leak in Xlib when using fonts in an international (I18N) environment. This problem affects Netscape Navigator in particular. • A potential security vulnerability has been discovered where under certain circumstances users may gain unauthorized access. DIGITAL has corrected this potential vulnerability.
Patch 699.00 OSF415-400437C	**Patch:** quota and edquota Command Corrections **State:** New. Supersedes patches OSF415-400122 (54.00), OSF415-405422 (628.00) This patch corrects the following: • Correct quota command to return most severe error status on exit. • Fixes a problem with the edquota utility, which prevented a user from creating quotas for UIDs or GIDs that did not already exist in the /etc/passwd or /etc/group files. • Fixes a problem in which the vquota, vedquota, quota, edquota, dump, csh, and nslookup commands will sometimes display incorrect error messages for non-English locales.
Patch 700.00 OSF415-400437D	**Patch:** dump and rdump Command Corrections **State:** Supersedes patches OSF415-400079 (44.00), OSF415-400382 (304.00) This patch corrects the following: • Fixes problems that occur with the dump and rdump commands. The commands will fail with the following error message: available blocks n < estimated blocks m When a member of group "operator" logged into the console and (r)dump was invoked with the -n flag, an extraneous file (/dev/:0) was created. • Fixes a problem in which the dump command fails when the full pathname of the output file is not given. • Fixes a problem in which the vquota, vedquota, quota, edquota, dump, csh, and nslookup commands will sometimes display incorrect error messages for non-English locales.

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

Patch 701.00	**Patch:** ksh Corrections
OSF415-400437E	**State:** New. Supersedes patches OSF415-400118 (52.00), OSF415-400169 (80.00), OSF415-410057 (16.00), OSF415-400270 (177.00), OSF415-400304 (198.00), OSF415-400326 (235.00), OSF415-400435 (326.00), OSF415-405301 (546.00), OSF415-405331 (565.00), OSF415-400193 (93.00), OSF415-400434 (325.00), OSF415-405343 (573.00), OSF415-405159 (409.00), OSF415-405365 (590.00), OSF415-405389 (609.00) This patch corrects the following: • Fixes a problem that occurs if the kernel tunable variable "old-obreak" is set to zero and the system is running the Korn shell (ksh). The shell gets caught in an infinite loop printing a message similar to the following. Eventually the process will core dump. /adp/bin/adpbkup[135]: no space • Fixes a problem with the ksh shell program. ksh prevents a command which runs in a sub-process from writing to a tape device. • Fixes a problem that occurs when using the Korn shell (ksh). Keyboard input is not echoed when a user exits via a trap, after editor options have been set in ksh. • Fixes a problem in which the ksh command periodically prints erroneous characters instead of the command that was typed. • Fixes a problem in which the ksh shell sometimes reverses the group id (GID) and the effective group id (egid) of the calling process. • Fixes problems that occur when using the ksh shell. When the PATH for a command is not found, the following error message is displayed. Also, when the set command is executed, the system core dumps. • Fixes a problem that occurs when using the Korn shell (ksh). Variables set with the typeset -L[n] built-in command do not work correctly when other subshells are spawned. • Fixes a problem that was caused by the Korn shell running in EMACS mode. When a window was resized with a width that exceeded 160 characters, the next command (or even a return) would cause the ksh utility to core dump. • Fixes a problem in the kornshell in which the "lt" operator didn't work correctly when the first expression was more than ten digits. • Fixes a problem when builtin variables (ex. TMOUT) are exported as readonly with values > 256. The 'set' command (display all variables) will cause ksh to core dump with the error "stack overflow". • Corrects several serious problems with the "csh" command. Some of these the commands under the "csh" shell. • Fixes a problem that occurs when using the C shell (csh). When a command that does both wildcard expansion and command substitution is run in csh, incorrect results are produced. • Fixes the problem that csh may omit the data byte 0x80 when processing a string in the ja_JP.SJIS or zh_TW.big5 locales.

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

Patch 701.00 continued	• Corrects a problem which results in a superuser being able to inadvertently bring the system down to single user mode by accidentally killing pid 1 (init) when trying to kill a background job (%1). • Fixes a memory managment problem that occurs on systems running the Korn shell. Incorrect results occur when the length of the parameter to the echo command is altered. • Fixes a problem in which the vquota, vedquota, quota, edquota, dump, csh, and nslookup commands will sometimes display incorrect error messages for non-English locales.
Patch 703.00 OSF415-410169C	**Patch:** AdvFS rmvol Command Fix **State:** New Fixes an AdvFS problem that occurs when the rmvol command is stopped before the commmand successfully removes a volume from a domain. As a result, the showfdmn and addvol commands interpreted the volume as still in the domain (although with no data available) and a balance operation returned the following AdvFS error message: get vol params error EBAD_VDI (-1030)
Patch 704.00 OSF415-405411B	**Patch:** clock_settime Correction, Static Library **State:** Supersedes patches OSF415-400215 (107.00), OSF415-400215B (491.00) This patch corrects the following: • When setting the date with the clock_settime rtl service routine, the date will not get past the date of 'Sat Sep 8 19:46:39 2001'. If you try to set past this date the routine returns a EINVAL error. • Fixes the following two problems with realtime library: – A locking problem when calling sem_close() with an invalid descriptor – A memory leak
Patch 706.00 OSF415-405407B	**Patch:** libpacl.a Static Library Fix **State:** New Corrects the problem with setacl not being able to handle a user ID beginning with a numeral.
Patch 707.00 OSF415X11-405011C	**Patch:** Security (SSRT0547U) **State:** New A potential security vulnerability has been discovered where under certain circumstances users may gain unauthorized access. DIGITAL has corrected this potential vulnerability.