DIGITAL UNIX and TruCluster Software

Patch Summary and Release Notes for DIGITAL UNIX 4.0A and TruCluster 1.4A, Patch Kit-0008

March 1999

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

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

Compaq Computer Corporation
Houston, Texas

Contents

About This Manual

This manual contains information specific to Patch Kit-0008 for the DIGITAL UNIX Version 4.0A operating system and TruCluster 1.4A software 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.

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

Related Documentation

In addition to this manual, you should be familiar with the concepts and mechanisms described in the following 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 4.0A and TCR 1.4A Patch Kit-0008.

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 ~46 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 ~47 MB of storage space in `/var/adm/patch` may be required for original files if you choose to install and revert all patches. See the *Patch Kit Installation Instructions* for more information.

  Up to ~94 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.

TruCluster Software products

- Temporary Storage Space

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

- Permanent Storage Space

  Up to ~51 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 ~52 MB of storage space in `/var/adm/patch` may be required for original files if you choose to install and revert all patches. See the *Patch Kit Installation Instructions* for more information.

  Up to ~1019 KB of storage space is required in `/var/adm/patch/doc` for patch abstract and README documentation.

  A total of ~120 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 4.0A and TCR1.4A installed follows:

- If a DIGITAL UNIX 4.0A Patch 1.00 is chosen for installation and it depends upon TruCluster 1.4A 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 4.0A 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 749.00

This patch modifies `/etc/ddr.dbase` and `/etc/ddr.db`. A copy of the original files should be made before installing this patch.

1.5 Release Note for Patch 694.00

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

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 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.

The cc driver interprets the -input_to_ld switch as a -input switch destined for ld, and places it on the ld command line in the same relative position that it had on the cc command line. This not only ensures that crt0.o is passed to the linker first, but also preserves the linking order that the user specified on the original cc command line.

1.6 Release Note for Patch 676.00

The following sections contain reference page updates.

1.6.1 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.

1.6.2 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)

1.6.3 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.

- o 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.

- o 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.

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

- o 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.

- o 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

1.7 Release Note for Patch 643.00

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.

1.8 Release Note for Patch 762.00

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.

1.9 Release Note for Patch 817.00

The updated reference page sections for `mount(8)` follow:

mount(8), 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.

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.

2

Summary of Base Operating System Patches

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

Table 2–1 lists patches that have been updated.

Table 2–2 provides a summary of patches in Patch Kit-0008.

Table 2–1: Updated Base Operating System Summary

Patch IDs	Change Summary
Patches 592.00, 593.00, 594.00, 598.00, 603.00, 615.00, 625.00, 633.00, 639.00, 651.00, 669.00, 677.00, 684.00, 695.00, 696.00, 706.00, 710.00, 711.00, 718.00, 726.00, 740.00, 741.00, 742.00, 772.00, 776.00, 777.00, 788.00, 791.00, 793.00	New
Patch 164.00	Superseded by Patch 247.02
Patch 339.00	Superseded by Patch 301.01
Patch 339.00	Superseded by Patch 305.01
Patch 100.00	Superseded by Patch 583.01
Patch 140.00	Superseded by Patch 595.00
Patch 180.00	Superseded by Patch 596.00
Patches 138.00, 139.00, 453.00, 455.00, 584.00	Superseded by Patch 597.00
Patches 145.00, 203.00, 286.00, 457.00, 575/00, 576.00, 599.00, 600.00, 601.00	Superseded by Patch 602.00
Patches 263.00, 320.00, 66.00, 511.00	Superseded by Patch 612.00
Patches 55.00, 76.00, 137.00, 343.00, 526.00	Superseded by Patch 619.00
Patch 474.00	Superseded by Patch 623.00
Patches 272.00, 484.00	Superseded by Patch 643.00
Patch 467.00	Superseded by Patch 648.00
Patch 136.00	Superseded by Patch 656.00
Patch 225.00	Superseded by Patch 660.00
Patches 176.00, 361.00	Superseded by Patch 667.00
Patch 158.00	Superseded by Patch 675.00
Patches 63.00, 377.00, 552.00	Superseded by Patch 676.00
Patches 184.01, 516.00	Superseded by Patch 689.00
Patches 419.00, 645.00	Superseded by Patch 694.00
Patches 264.00, 606.00	Superseded by Patch 697.00
Patches 227.00, 502.00	Superseded by Patch 705.00
Patch 407.00	Superseded by Patch 708.00

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

Patch 478.00	Superseded by Patch 709.00
Patches 86.00, 42.00	Superseded by Patch 713.00
Patch 167.00	Superseded by Patch 723.00
Patches 131.00, 411.01	Superseded by Patch 731.00
Patches 281.00, 401.00, 485.00	Superseded by Patch 736.00
Patches 56.00, 70.00, 75.00, 83.00, 111.00, 114.00, 117.00, 125.00, 126.00, 164.00, 65.00, 205.00, 92.00, 110.00, 168.00, 183.00, 202.00, 223.00, 230.00, 239.00, 278.00, 282.00, 339.00, 339.01, 316.00, 321.00, 324.00, 329.00, 342.00, 355.00, 356.00, 362.00, 365.00, 372.00, 394.00, 413.00, 424.00, 425.00, 476.00, 479.00, 487.00, 494.00, 498.00, 501.00, 519.00, 499.00, 173.00, 100.00, 475.00, 624.00, 654.00, 657.00, 661.00, 663.00, 680.00, 686.00, 716.00, 717.00, 727.00, 725.00, 102.00, 133.00, 213.00, 261.00, 279.00, 319.00, 416.00, 649.00, 671.00, 166.00, 415.00, 681.00, 508.00, 701.00, 73.00, 33.00, 104.00, 304.00, 751.00, 78.00, 391.00, 644.00, 784.00, 795.00	Superseded by Patch 737.00
Patches 64.00, 71.00, 71.01, 128.01	Superseded by Patch 739.00
Patch 189.01	Superseded by Patch 743.00
Patch 233.00	Superseded by Patch 744.00
Patches 177.00, 611.00, 745.00	Superseded by Patch 748.00
Patches 67.00, 238.00, 221.00, 208.00, 193.00, 252.00, 308.00, 712.00	Superseded by Patch 749.00
Patch 572.00	Superseded by Patch 759.00
Patches 80.00, 90.00, 98.00, 107.00, 25.00, 58.00, 60.00, 91.00, 99.00, 34.00, 36.00, 37.00, 38.00, 40.00, 116.00, 129.00, 170.00, 174.00, 155.00, 160.00, 171.00, 186.00, 195.00, 48.00, 94.00, 45.00, 220.00, 172.00, 29.00, 31.00, 44.00, 52.00, 53.00, 187.00, 162.00, 222.00, 197.00, 182.00, 59.00, 196.00, 200.00, 190.00, 212.00, 211.00, 185.00, 217.00, 224.00, 229.00, 226.00, 258.00, 231.00, 271.00, 276.00, 277.00, 219.00, 109.00, 242.00, 253.00, 300.00, 274.00, 262.00, 265.00, 267.00, 293.00, 325.00, 328.00, 329.00, 330.00, 331.00, 332.00, 333.00, 352.00, 376.00, 374.00, 360.00, 358.00, 375.00, 268.00, 87.00, 359.00, 366.00, 357.00, 363.00, 290.00, 303.00, 312.00, 369.00, 207.00, 380.00, 382.00, 383.00, 463.00, 386.00, 387.00, 460.00, 379.00, 400.00, 403.00, 404.00, 405.00, 420.00, 427.00, 421.00, 430.00, 433.00, 438.00, 370.00, 441.00, 465.00, 477.00, 486.00, 488.00, 489.00, 509.00, 513.00, 515.00, 518.00, 521.00, 524.00, 525.00, 533.00, 534.00, 536.00, 541.00, 542.00, 546.00, 548.00, 550.00, 551.00, 562.00, 563.00, 571.00, 580.00, 581.00, 514.00, 492.00, 604.00, 605.00, 613.00, 618.00, 621.00, 622.00, 626.00, 628.00, 629.00, 630.00, 637.00, 638.00, 640.00, 641.00, 650.00, 652.00, 658.00, 664.00, 666.00, 670.00, 674.00, 678.00, 679.00, 683.00, 685.00, 688.00, 690.00, 691.00, 692.00, 693.00, 698.00, 700.00, 702.00, 703.00, 704.00, 707.00, 714.00, 715.00, 719.00, 720.00, 728.00, 729.00, 730.00, 732.00, 738.00, 750.00, 755.00, 756.00, 757.00, 761.00, 490.00, 538.00, 773.00, 620.00, 687.00, 647.00, 653.00, 724.00, 746.00, 753.00, 699.00, 765.00, 767.00, 769.00, 775.00, 768.00, 771.00, 668.00	Superseded by Patch 760.00
Patches 23.00, 119.00, 218.00, 317.00, 340.00, 559.00, 51.00, 255.00, 464.00, 28.00, 241.00, 385.00, 555.00, 752.00, 758.00	Superseded by Patch 762.00

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

Patch 69.01	Superseded by Patch 774.00
Patch 134.00	Superseded by Patch 778.00
Patches 152.00, 289.00, 367.00	Superseded by Patch 781.00
Patch 69.01	Superseded by Patch 774.00
Patches 214.00, 215.00, 782.00	Superseded by Patch 783.00
Patches 138.00, 139.00, 453.00, 455.01	Superseded by Patch 785.00
Patch 209.00	Superseded by Patch 786.00
Patches 189.00, 587.00	Superseded by Patch 789.00
Patches 152.00, 289.00, 367.00	Superseded by Patch 792.00
Patch 69.01	Superseded by Patch 774.00
Patches 135.00, 169.00, 257.00, 395.00, 123.00, 397.00, 586.00	Superseded by Patch 796.00
Patches 164.00, 246.00, 246.01, 283.00, 406.00	Superseded by Patch 798.00
Patch 69.01	Superseded by Patch 774.00
Patch 154.00	Superseded by Patch 801.00
Patch 154.00	Superseded by Patch 802.00
Patch 339.00, 302.01	Superseded by Patch 803.00
Patches 339.00, 302.01	Superseded by Patch 804.00
Patches 452.00, 545.00	Superseded by Patch 805.00
Patch 452.00, 545.00	Superseded by Patch 806.00
Patch 348.00	Superseded by Patch 807.00
Patch 348.00	Superseded by Patch 808.00
Patches 216.00, 349.00, 577.00, 780.00	Superseded by Patch 809.00
Patches 440.00, 390.01	Superseded by Patch 811.00
Patches 393.00, 118.00, 122.00, 393.01, 482.00, 495.00, 631.00	Superseded by Patch 813.00
Patches 393.00, 118.00, 122.00, 393.01, 482.00, 495.00, 631.00	Superseded by Patch 814.00
Patches 72.00, 62.00, 77.00, 82.00, 93.00, 113.00, 194.00, 232.00, 269.00, 270.00, 398.00, 408.00, 414.00, 436.00, 480.00, 507.00, 510.00, 532.00, 537.00, 560.00, 493.00, 523.00, 614.00, 642.00	Superseded by Patch 815.00
Patches 72.00, 62.00, 77.00, 82.00, 93.00, 113.00, 194.00, 232.00, 269.00, 270.00, 398.00, 408.00, 414.00, 436.00, 480.00, 507.00, 510.00, 532.00, 537.00, 560.00, 493.00, 523.00, 614.00, 642.00	Superseded by Patch 816.00

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

Patches 32.00, 95.00, 120.00, 105.00, 155.00, 157.00, 157.01, 192.00, 206.00, 240.00, 210.00, 236.00, 250.00, 104.00, 251.00, 292.00, 327.00, 307.00, 310.00, 371.00, 388.00, 462.00, 461.00, 392.00, 423.00, 444.00, 445.00, 472.00, 422.00, 578.00, 569.00, 450.00, 450.01, 483.00, 491.00, 496.00, 505.00, 522.00, 528.00, 530.00, 531.00, 535.00, 539.00, 540.00, 543.00, 544.00, 549.00, 558.00, 565.00, 568.00, 569.00, 570.00, 553.00, 608.00, 610.00, 627.00, 632.00, 634.00, 635.00, 636.00, 646.00, 655.00, 665.00, 673.00, 682.00, 721.00, 733.00, 734.00, 747.00, 754.00, 764.00, 770.00, 779.00, 763.00, 506.00, 609.00, 787.00, 672.00, 722.00, 790.00, 794.00	Superseded by Patch 817.00
Patches 32.00, 95.00, 120.00, 105.00, 155.00, 157.00, 157.01, 192.00, 206.00, 240.00, 210.00, 236.00, 250.00, 104.00, 251.00, 292.00, 327.00, 307.00, 310.00, 371.00, 388.00, 462.00, 461.00, 392.00, 423.00, 444.00, 445.00, 472.00, 422.00, 578.00, 569.00, 450.00, 450.01, 483.00, 491.00, 496.00, 505.00, 522.00, 528.00, 530.00, 531.00, 535.00, 539.00, 540.00, 543.00, 544.00, 549.00, 558.00, 565.00, 568.00, 569.00, 570.00, 553.00, 608.00, 610.00, 627.00, 632.00, 634.00, 635.00, 636.00, 646.00, 655.00, 665.00, 673.00, 682.00, 721.00, 733.00, 734.00, 747.00, 754.00, 764.00, 770.00, 779.00, 763.00, 506.00, 609.00, 787.00, 672.00, 722.00, 790.00, 794.00	Superseded by Patch 818.00
Patches 339.01, 274.00, 230.00, 164.00, 229.00, 272.00, 797.00, 799.00	Superseded by Patch 819.00
Patches 339.01, 274.00, 230.00, 164.00, 229.00, 272.00, 797.00, 799.00	Superseded by Patch 820.00
Patch 54.00	Superseded by Patch 821.00
Patch 54.00	Superseded by Patch 822.00
Patches 454.00, 591.00	Superseded by Patch 823.00
Patch 454.01	Superseded by Patch 824.00

Table 2–2: Summary of Base Operating System Patches

Patch IDs	Abstract
Patch 61.00 OSF405-400058	**Patch:** gated Daemon Corrections **State:** Existing This patch allows a system that is running 'gated' to update internal routing tables to manage the router discovery function.
Patch 74.00 OSF405-400074	**Patch:** Security, rlogin (SSRT0416U) **State:** Existing A potential security vulnerability has been discovered in "rlogin", where under certain circumstances users may gain unauthorized access. DIGITAL has corrected this potential vulnerability.
Patch 79.00 OSF405-400081	**Patch:** ZLXp-L1 or ZLXp-L2 Graphics Option Corrections **State:** Existing This patch corrects the following ZLXp-L1 or ZLXp-L2 graphics option problems: • Stereo mode (XStereo) does not function properly. • Applications that use the second hardware colormap do not display the correct colors.

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

Patch 84.00 OSF405-400089	**Patch:** Security, ris_pax (SSRT0413U) **State:** Existing A potential security vulnerability has been discovered in 'ris_pax', where under certain circumstances users may gain unauthorized access. DIGITAL has corrected this potential vulnerability.
Patch 88.00 OSF405-400095	**Patch:** FDDI DEMFA Driver Corrections **State:** Existing This patch fixes a halt/restart problem with the FDDI DEMFA driver when the interface performs the ESP self tests.
Patch 101.00 OSF405-400117	**Patch:** Ping Command Timeout Correction **State:** Existing Ping command can time out after invoking the "rcinet restart" command.
Patch 106.00 OSF405-400126	**Patch:** Kernel Memory Fault in dqget() Routine Correction **State:** Existing This patch fixes a "kernel memory fault" in the dqget() routine.
Patch 108.00 OSF405-400128	**Patch:** Corrections For Various Keyboards **State:** Supersedes patch OSF405-039 (39.00) This patch corrects the following: • Issuing a SET_DEVICE_MODE ioctl to the workstation driver to change cursor reporting to relative mode fails. • On systems with PCXAL, LK411, and similar keyboards, sometimes on boot or between sessions on the workstation monitor, the keyboard stops working.
Patch 115.00 OSF405-400140	**Patch:** ATI Mach64 Graphics Card Monitor Handling, GRDRIVER **State:** Existing On systems with an ATI Mach64 graphics card, sometimes the monitor goes into power-save mode and cannot be restored.
Patch 130.00 OSF405-400166	**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 132.00 OSF405-400168	**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 141.00 OSF405DX-400001	**Patch:** dxsysinfo Corrections **State:** Existing This patch corrects the following problems: • dxsysinfo causes the X server's colormap entries to be corrupted. • dxsysinfo may display certain filesystem percent full values incorrectly. • dxsysinfo repeatedly adds device /dev/prf as a tape entry into its Device Information Area. • dxsysinfo leaves its child process orphaned after a logout. • Hard disk icons fail to display in the Device Information Area when the colormap is full or on a black/white screen.

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

Patch 142.00 OSF405DX-400002	**Patch:** dxterm Support To Suppress ANSI Escape Sequences **State:** Existing This patch adds the new resource printOnlyPrintables to dxterm. When this resource is set to TRUE (the default is FALSE), dxterm will not output any escape sequences when printing. This is needed for some PostScript printer (filters) that can not handle escape sequences.
Patch 159.00 OSF405-400179	**Patch:** CD/DSR Not Dropping Right Away After Dial-out **State:** Existing uugetty - corrects CD/DSR not dropping right away after dial-out.
Patch 161.00 OSF405-400183	**Patch:** rwhod Correction **State:** Existing This patch fixes a problem in which rwhod daemon can cause a core dump with a segmentation fault.
Patch 165.00 OSF405-400191	**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 178.00 OSF405-400206	**Patch:** tic Command Correction **State:** Existing This patch fixes a problem in which the tic command incorrectly returns a non-zero exit value upon successful completion. An exit value of 0 should be returned upon successful completion.
Patch 191.00 OSF405DX-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 198.00 OSF405-063	**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 199.00 OSF405-400223	**Patch:** talkd Correction, Security (SSRT0446U) **State:** Existing A potential security vulnerability in talkd has been corrected.
Patch 204.00 OSF405CDE-400009	**Patch:** dtksh Command Correction **State:** Existing This patch 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

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

Patch 243.00 OSF405-400263	**Patch:** ar Command Correction **State:** Supersedes patch OSF405-400046 (57.00) This patch corrects the following: • The ar command's -x option, which extracts objects from archive files, may incorrectly output a message stating that the file was not found. • 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 userd). – 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
Patch 247.02 OSF405-400189C-2	**Patch:** uucp Command Correction, (SSRT0296U) **State:** Supersedes patch OSF405-400189 (164.00) 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.
Patch 248.00 OSF405-087	**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
Patch 249.00 OSF405-095	**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 <carriage return> that exceeds 255 characters. In some cases, characters will be truncated.
Patch 254.01 OSF405-099-1	**Patch:** S3 Trio64V+ Graphics Card Incorrectly Identified **State:** Existing The S3 Trio64V+ graphics card (PB2GA-JC or PB2GA-JD) is not being uniquely identified by the driver at startup.
Patch 256.00 OSF405-101	**Patch:** PowerStorm 4D20 Graphics Option Monitor Resolution **State:** Supersedes patch OSF405-024 (24.00) This patch corrects the following: • On systems with a PowerStorm 4D20 (TGA2) graphics option, monitor resolution setting 4 (1600x1200 at 65 Hz) is not set up properly. • AlphaStation 255 systems with a PowerStorm 3D30 (PBXGB-AA) or PowerStorm 4D20 (PBXGB-CA) graphics card may hang, halt, or crash.

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

Patch 259.00 OSF405-400268	**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 260.00 OSF405-400269	**Patch:** Commands, Shells, & Utility Patches **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 266.00 OSF405-400282	**Patch:** quotas For Filesystems Causes rpc.rquotad To Hang **State:** Supersedes patch OSF405-400214 (188.00) 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 275.00 OSF405-400295	**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 280.00 OSF405-400305	**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 288.01 OSF405X11-400016-1	**Patch:** S3 Trio64 Graphics Card Can Lose Time **State:** Supersedes patch OSF405X11-400011 (153.00) This patch corrects the following: • Systems with an S3 Trio64 graphics card can lose time (on the order of a few minutes a day). • On systems with an S3 Trio64V+ graphics card (PB2GA-JC or PB2GA-JD), the X server hangs while drawing the login screen.

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

Patch 296.00 OSF405-105	**Patch:** System Crash With >1GB Of Memory **State:** Supersedes patch OSF405-027 (27.00) This patch corrects the following: • AlphaServer 2100A systems crash during boot with greater than 1GB of memory installed. • 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 301.01 OSF405-400331B-1	**Patch:** uusend And uustat Command Correction **State:** Supersedes patch OSF405-400331 (339.00) 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 305.01 OSF405-400331D-1	**Patch:** voliod Command Correction **State:** Supersedes patch OSF405-400331 (339.00) 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 309.00 OSF405-113	**Patch:** io_zero() Incorrect Value On AlphaServer 1000 **State:** Existing This patch fixes a problem in which the io_zero() system call returns an incorrect value on an AlphaServer 1000.
Patch 313.00 OSF405-117	**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 318.00 OSF405-400325	**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.
Patch 322.00 OSF405-400337	**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 323.00 OSF405-400340	**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.

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

Patch 334.00 OSF405-400358	**Patch:** awk Utility Correction **State:** Supersedes patch OSF405-400318 (294.00) This patch corrects the following: • Fixes problem in which 'awk' consumes 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 335.00 OSF405-400359	**Patch:** auditmask Utility Correction **State:** Existing 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 336.01 OSF405-400362-1	**Patch:** libm (shared library) Corrections **State:** Supersedes patch OSF405-400083 (81.00), OSF405-400293 (273.00) 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 337.01 OSF405-400364-1	**Patch:** System Run Level Correction **State:** Existing This patch corrects the following: • 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 338.01 OSF405-400365-1	**Patch:** btree File Format Static Library Correction **State:** Existing This patch fixes a problem 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 341.00 OSF405-400370	**Patch:** Correction To volunroot, volrootmir, vol-reconfig **State:** Existing This patch fixes several LSM problems related to the volunroot, volrootmir, and vol-reconfig scripts.

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

Patch 344.01 OSF405-400371-1	**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 345.00 OSF405CDE-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 346.00 OSF405DX-400012	**Patch:** Bookreader Corrections, (SSRT0514U) **State:** Supersedes patch OSF405DX-400003 (143.00) This patch corrects the following: • Bookreader aborts with a segmentation fault when displaying certain pages if the required fonts are not available. This problem usually occurs when redirecting Bookreader's display to another vendor's workstation (HP or Sun). • 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 347.00 OSF405X11-400018	**Patch:** X server Correction **State:** Existing The X server can loop or run out of sockets when dealing with a font server.
Patch 350.00 OSF405-400383	**Patch:** Correction To llogin Command **State:** Existing This patch 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 351.00 OSF405-400377	**Patch:** Packets Out of Order On PATHWORKS Netbuei clients **State:** Supersedes patch OSF405-400097 (89.00) This patch corrects the following: • Corrects a problem with packets out of order experienced by some PATHWORKS Netbuei clients. • 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 378.01 OSF405-400406-1	**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 381.00 OSF405-127	**Patch:** Token Ring Transmission Timeout **State:** Supersedes patches OSF405-043 (43.00), OSF405-043-1 (43.01) This patch corrects the following: • Fixes a Token Ring transmission timeout. The driver can experience "ID 380PCI20001 (8/13/95)" as described in the TI380PCI Errata. • This patch is an upgrade/replacement for the Token Ring driver. 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 384.00 OSF405-135	**Patch:** Cortex Platform Support, VME Interrupt Failure **State:** Supersedes patch OSF405-050 (50.00) This patch corrects the following: • Fixes a bug in the the Cortex platform support code (ebv14.c) where the handler_dsabl() function for VME interrupts fails if more than one SCB vector has interrupts installed for the same IRQ priority level. • 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
Patch 402.00 OSF405-400416	**Patch:** who Command Correction **State:** Existing This patch 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 410.00 OSF405-400427	**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 412.00 OSF405-400429	**Patch:** pcnfsd Correction **State:** Existing This patch provides the following 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 418.00 OSF405-400438	**Patch:** egfaults In nm For C++ Compiler Correction **State:** Existing This patch fixes segfaults in nm for object files generated by the C++ compiler.

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

Patch 429.00 OSF405-400455	**Patch:** ex Command Correction **State:** Existing This patch 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
Patch 431.00 OSF405-400457	**Patch:** pax tar And cpio Archive Handling Correction **State:** Supersedes patches OSF405-400258 (235.00), OSF405-400320 (315.00), OSF405-400374 (353.00), OSF405-400395 (396.00) This patch corrects the following: • Fix pax's tar and cpio archive handling to allow filesizes 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 the following problems with the pax command when cpio format is used: – The cpio -z command hangs the system when small files are read using a large block size. – When reading a series of commands, cpio fails on the second command and displays a "No input" error message. If an identical third cpio read is issued, cpio works as expected. • 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 437.00 OSF405-400465	**Patch:** OSF405-400465 **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.

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

Patch 443.00 OSF405-400473	**Patch:** GEMC Compiler Corrections **State:** Supersedes patches OSF405-400091 (85.00), OSF405-400149 (121.00), OSF405-400187 (163.00), OSF405-400257 (234.00) 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. • Fixes a problem where the DEC C compiler would hang when compiling files containing many thousands of #line directives. • The compiler generates 8 bytes of return code for functions that are defined to return a 4-byte structure. • A non-standard use of the __builtin_va_start compiler builtin was causing the compiler to crash. • The compiler preprocessor was incorrectly issuing a warning diagnostic on the use of an octal constant. • The compiler was not issuing a diagnostic for the use of the "long double" datatype. • Corrects the following 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.
Patch 447.00 OSF405-400478	**Patch:** LAT Correction **State:** Supersedes patch OSF405-400107 (97.00) This patch corrects the following: • Corrects a problem where processes such as wall, ntalkd, and comsat, when associated with LAT devices, get stuck in the 'u' state (processes are hung) and cannot be cleared from the system. • 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 456.00 OSF405CDE-400015	**Patch:** Security, (SSRT0431U, SSRT0525U) **State:** Supersedes patch OSF405CDE-400008 (181.00) 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.

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

Patch 459.00 OSF405DX-400015	**Patch:** Security, (SSRT0435U) **State:** Supersedes patches OSF405DX-400006 (175.00), OSF405DX-400009 (285.00), OSF405DX-400011 (287.00) 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 OSF405DX-400006 installed. The dop command rejects all password attempts when run by non-root users. • Fixes a problem that occurs on systems that have installed Patch OSF405DX-400006. If more than one argument is given on the dop command line, dop passes all arguments as a single argument to the command. • This patch 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. – When Enhanced Security is enabled, userdel command incorrectly removes an account from /etc/passwd. • The startup of nissetup, latsetup and btcreate /etc/doprc entries via the dop command fails with exit code of 2.
Patch 466.00 OSF405-078	**Patch:** DLI Application Correction **State:** Existing This patch fixes a problem that prevented DLI applications from working over funneled drivers.
Patch 473.00 OSF405X11-008	**Patch:** Memory Leak X server Correction **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 graphics card.
Patch 481.00 OSF405-154	**Patch:** sort Command Corrections **State:** Existing Fixes the error condition that the sort command may erroneously skip 8-bit characters when the -d or -i option is specified.

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

Patch 504.00 OSF405-193	**Patch:** Security, (SSRT0456U), rpc.statd Correction **State:** Supersedes patches OSF405-400412 (399.00), OSF405-400412-1 (399.01) 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 behavior). Also, this patch catches and logs other signals that would otherwise make rpc.statd disappear without a trace.
Patch 512.00 OSF405-208	**Patch:** FDDI Driver Correction **State:** Supersedes patches OSF405-400225 (201.00), OSF405-400409 (364.00), OSF405-400467 (439.00) This patch corrects the following: • This patch is 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. • Resolves a problem in the FDDI driver during device reset and initialization. • Fixes a kernel memory fault caused by the fta FDDI driver. • Corrects a problem with the FDDI fta driver.
Patch 527.00 OSF405-211	**Patch:** /sbin/loader Corrections **State:** Supersedes patch OSF405-400152 (124.00) This patch corrects the following: • Fixes a problem that may cause /sbin/loader to fail to resolve duplicate symbols in dlopen'ed shared libraries. • This patch 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 529.00 OSF405-218	**Patch:** Correction to the -s option of ncheck Utility **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 547.00 OSF405-244	**Patch:** kdbx, mbuf, and socket Extension Corrections **State:** Existing This patch corrects a problem with the kdbx mbuf and socket extensions. The use of these extension on some crashdumps resulted in errors and would hang.

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

Patch 566.00 OSF405-227	**Patch:** mountd Correction, Security (SSRT0496U) **State:** Supersedes patches OSF405-400343 (326.00), OSF405-201 (503.00) 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.
Patch 567.00 OSF405-255	**Patch:** Provides filterlog Command **State:** Supersedes patch OSF405-213 (517.00) 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 573.00 OSF405CDE-003	**Patch:** dtbuilder Segmentation Fault Correction **State:** Supersedes patch OSF405CDE-400010 (284.00) 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 574.00 OSF405CDE-004	**Patch:** xset Command Correction **State:** Existing This patch fixes a problem where the xset command could not clear the screen saver under CDE.
Patch 583.01 OSF405-400203B-1	**Patch:** auth_for_terminal() Segmentation Fault Correction **State:** Supersedes patch OSF405-400115 (100.00) 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.

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

Patch 585.00 OSF405-400362B	**Patch:** libm (static library) Corrections **State:** Supersedes patches OSF405-400083 (81.00), OSF405-400293 (273.00), OSF405-400362 (336.00) 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 588.00 OSF405-400364B	**Patch:** System Storage Run Level Correction **State:** Supersedes patch OSF405-400364 (337.00) This patch corrects the following: • 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 589.00 OSF405-400365B	**Patch:** btree File Format Correction **State:** Supersedes patch OSF405-400365 (338.00) This patch fixes a problem 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 590.00 OSF405-400371B	**Patch:** uprofile And Kprofile Development Corrections **State:** Supersedes patch OSF405-400371 (344.00) 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 592.00 OSF405CDE-010	**Patch:** rpc.cmsd and dtcm Corrections **State:** New This patch 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. These invalid entries would include "remove" entries that specify non-existent keys. • Repeating appointments with a frequency of daily are sometimes displayed incorrectly by the calendar manager (dtcm). Some appointments are displayed an hour earlier or an hour later than originally scheduled. • 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.

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

Patch 593.00 OSF405CDE-011	**Patch:** dtmail Command Correction **State:** New This patch fixes a problem where dtmail can core dump when there exists long lines in Sun Mail Tool attachments. This causes a buffer overflow.
Patch 594.00 OSF405CDE-005	**Patch:** dxkeyboard Application Modification **State:** New This patch 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.
Patch 595.00 OSF405CDE-006	**Patch:** Window Manager Correction **State:** Supersedes patch OSF405CDE-400005 (140.00) This patch fixes 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 596.00 OSF405CDE-007	**Patch:** Security, (SSRT0438U) **State:** Supersedes patch OSF405CDE-400007 (180.00) This patch fixes 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 597.00 OSF405CDE-008A	**Patch:** dtterm Corrections **State:** Supersedes patches OSF405CDE-400003 (138.00), OSF405CDE-400004 (139.00), OSF405CDE-400012 (453.00), OSF405CDE-400014 (455.00), OSF405CDE-400014B (584.00) 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. • Prevents the escape sequence that sets DECterm window titles from hanging dtterm windows. • 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.

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

Patch 598.00 OSF405CDE-009	**Patch:** Fix for Calender Manager (dtcm) Hang **State:** New This patch 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.
Patch 602.00 OSF405DX-008	**Patch:** Account Management Command Correction **State:** Supersedes patches OSF405DX-400005 (145.00), OSF405DX-400008 (203.00), OSF405DX-400010 (286.00), OSF405DX-400013 (457.00), OSF405DX-004 (575.00), OSF405DX-003 (576.00), OSF405DX-005 (599.00), OSF405DX-006 (600.00), OSF405DX-007 (601.00) 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. • This patch 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 and usermod does not correctly lock and unlock an account. – When Enhanced Security is enabled, userdel command incorrectly removes an account from /etc/passwd. • Fixes the following problems encountered when using the Account Manager application (dxaccounts): – When moving an accounts home directory, symbolic links in the old home directory are resolved and files pointed to by the links are copied into the new home directory. – The userdel utility core dumps when attempting to delete a user account that is running enhanced C2 security. – 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.

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

Patch 602.00 continued	• 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. • 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 603.00 OSF405DX-009	**Patch:** Fix for dxdiff Core Dump **State:** New This patch fixes a problem where dxdiff will core dump when comparing files with long lines.
Patch 612.00 OSF405-258	**Patch:** statfs Function Correction **State:** Supersedes patches OSF405-400275 (263.00), OSF405-400330 (320.00), OSF405-400065 (66.00), OSF405-186 (511.00) 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 a problem that occurs when the system experiences a very high volume of SNMP trap requests, some SNMP traps may be lost. • 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.

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

Patch 615.00 OSF405-262	**Patch:** ed -G Option Prints Extra Characters **State:** New This patch fixes a problem in which the ed command when used with the -G option prints extra characters.
Patch 619.00 OSF405-266	**Patch:** Linker Corrections **State:** Supersedes patches OSF405-400038 (55.00), OSF405-400077 (76.00), OSF405-400174 (137.00), OSF405-400375 (343.00), OSF405-212 (526.00) This patch corrects the following: • Fixes a problem where use of "ld -r" will change symbol preemption behavior. • Changes how the linker handles permission problems with chmod(), corrects an internal linker hang, and removes an unnecessary data segment boundary check for OMAGIC (impure) object files. • A performance problem that the linker has with hidden symbols (-hidden flag) and large numbers of shared library files (.so files). • 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 error diagnostics. • Fixes 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.
Patch 623.00 OSF405-271	**Patch:** AlphaStation 255 Hang on Reboot Correction **State:** Supersedes patch OSF405-150 (474.00) This patch fixes the following problems: • 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. The driver would send a REJECT message when the offset was zero and the time period was too slow. The REJECT was unnecessary, and furthermore, it caused the jukebox to fail.
Patch 625.00 OSF405-273	**Patch:** AdvFS Boot Correction **State:** New This patch fixes a problem in which AdvFS boot code has trouble traversing symbolic links.
Patch 633.00 OSF405-282A	**Patch:** rmvol Command Correction **State:** New This patch 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)

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

Patch 639.00 OSF405-290	**Patch:** last Command Fix **State:** New This patch 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.
Patch 643.00 OSF405-295	**Patch:** lpd Line Printer daemon Correction **State:** Supersedes patches OSF405-400290 (272.00), OSF405-157 (484.00) This patch corrects the following: • Fixes a problem where the lpq command causes the program to crash (Memory fault). • 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 fails to start. The error message from syslog is: /usr/spool/lpd.lock: locking failed: Operation would block • Fixes to improve the reliability and efficiency of DIGITAL UNIX print services.
Patch 648.00 OSF405-300	**Patch:** find Command Correction **State:** Supersedes patch OSF405-400379 (467.00) This patch fixes 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 651.00 OSF405-303	**Patch:** AlphaServer 1000A Kernel Memory Fault Fix **State:** New This patch fixes the following problems that occur on AlphaServer 1000A 4/233 and 4/266 systems. • If a machine check occurs, the register data written to the binary.errlog will show zeroes in all registers when viewed with DECevent. • If a correctable memory error occurs, the system panics with a kernel memory fault.
Patch 656.00 OSF405-311	**Patch:** Mail, mailx Command Correction, Security (SSRT0587U) **State:** Supersedes patche OSF405-400172 (136.00) This patch fixes the following problems: • Fixes 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 660.00 OSF405-315	**Patch:** kloadsrv May Cause System Panic **State:** Supersedes patch OSF405-400243 (225.00) This patch fixes the following problems: • 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 667.00 OSF405-327	**Patch:** ex and vi Editor Corrections **State:** Supersedes patches OSF405-400204 (176.00), OSF405-400390 (361.00) 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 with the vi editor environment variable EXINIT that occurs when EXINIT includes the editors so subcommand.
Patch 669.00 OSF405-329	**Patch:** tip Command Correction (SSRT0548U, SSRT0412U) **State:** New. Supersedes patch OSF405-264 (617.00) This patch fixes 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 675.00 OSF405-336	**Patch:** LEX Correction **State:** Supersedes patch OSF405-400177 (158.00) This patch fixes the following problems: • Fixes a LEX problem. Without this patch, LEX rejects quoted regular expressions where the ending quote is preceded by a double 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 676.00 OSF405-337	**Patch:** Security, (SSRT0487U) **State:** Supersedes patches OSF405-400061 (63.00), OSF405-400404 (377.00), OSF405-233 (552.00) This patch fixes the following problems: • 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. • Fixes a problem that occurs on multiprocessor machines in which the 'at' command causes extra batch jobs to be executed. Sometimes temporary files are created and not removed, causing the queue limit to be exceeded. • 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. • Corrects several problems with the "at", "cron", and "crontab" commands.
Patch 677.00 OSF405-338	**Patch:** Line Printer Performance Fix **State:** New This patch fixes a problem with the performance of some line printers on a 4100 cpu.
Patch 684.00 OSF405-346	**Patch:** Machine Server System Call Incorrect Type Check **State:** New This patch fixes a problem where the machine server system calls are not being type checked properly potentially causing system crashes by unprivileged programs.
Patch 689.00 OSF405-353	**Patch:** dd Command Correction **State:** Supersedes patches OSF405-400211-1 (184.01), OSF405-195 (516.00) 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, 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.

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

Patch 694.00 OSF405-358	**Patch:** Default C Compiler Correction **State:** Supersedes patches OSF405-400439 (419.00), OSF405-297 (645.00) This patch fixes 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 695.00 OSF405-359	**Patch:** advscan Data Corruption Fix **State:** New. Supersedes patch OSF405-263 (616.00) This patch fixes 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.
Patch 696.00 OSF405-360	**Patch:** expr Command Correction **State:** New This patch fixes a problem with the expr command in which the leading zeros are truncated if CMD_ENV is set to bsd.
Patch 697.00 OSF405-361	**Patch:** faa FDDI Driver Kernel Memory Fault Correction **State:** Supersedes patches OSF405-400280 (264.00), OSF405-196 (606.00) This patch fixes the following problems: • 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.

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

Patch 705.00 OSF405-369	**Patch:** rpc.lockd Corrections **State:** Supersedes patches OSF405-400246 (227.00), OSF405-178 (502.00) This patch corrects the following: • Patch addresses various rpc.lockd problems. • 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. – An NFS mounted file system may hang. – 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 • 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 706.00 OSF405-370	**Patch:** Process Hang When Calling flock **State:** New This patch 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 a flock() on the same file.
Patch 708.00 OSF405-372	**Patch:** rdist Utility Correction **State:** Supersedes patch OSF405-400424 (407.00) This patch fixes 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 709.00 OSF405-373	**Patch:** Console Terminal Panic Print Correction **State:** Supersedes patch OSF405-144 (478.00) This patch fixes the following: • 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.
Patch 710.00 OSF405-374	**Patch:** automount daemon Correctionautomount daemon Correction **State:** New This patch fixes an automount problem. An automount map file entry that included a comment was being parsed incorrectly, resulting in an error.

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

Patch 711.00 OSF405-375	**Patch:** rmfdmn command Correction **State:** New. Supersedes patch OSF405-314 (659.00) This patch fixes 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 713.00 OSF405-377	**Patch:** Pseudo TTY Corrections **State:** Supersedes patches OSF405-400092 (86.00), OSF405-042 (42.00) This patch corrects the following: • A problem where a remote user will kill rlogin or telnet and the server host will have an orphaned 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. • System causes an "assert_wait" panic and the stack contains streams modules. • Fixes a panic caused by freeing a pty on a reopen of the controlling tty.
Patch 718.00 OSF405-382	**Patch:** showfile Cmd Incorrectly Returns Error Status **State:** New This patch 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 723.00 OSF405-387	**Patch:** cron Command Correction **State:** Supersedes patch OSF405-400194 (167.00) This patch fixes 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 726.00 OSF405-390	**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. • Provides diskx with the ability to test 9 Gigabyte drives and provides added flexibility in diagnosing hardware problems.

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

Patch 731.00 OSF405-395	**Patch:** Security (SSRT0448U) **State:** Supersedes patches OSF405-400167 (131.00), OSF405-400428-1 (411.01) 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 736.00 OSF405-402	**Patch:** syslogd Correction (SSRT0499U) **State:** Supersedes patches OSF405-400306 (281.00), OSF405-400415 (401.00), OSF405-151 (485.00) 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. • 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 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. • 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 737.00 OSF405-403A	**Patch:** Library Patches, Security (SSRT0425U), (SSRT0296U) **State:** Supersedes patches OSF405-400039 (56.00), OSF405-400070 (70.00), OSF405-400076 (75.00), OSF405-400088 (83.00), OSF405-400106 (96.00), OSF405-400119 (103.00), OSF405-400133 (111.00), OSF405-400139 (114.00), OSF405-400143 (117.00), OSF405-400153 (125.00), OSF405-400154 (126.00), OSF405-400189 (164.00), OSF405-400064 (65.00), OSF405-400227 (205.00), OSF405-400101 (92.00), OSF405-400131 (110.00), OSF405-400195 (168.00), OSF405-400210 (183.00), OSF405-400226 (202.00), OSF405-400241 (223.00), OSF405-400239 (230.00), OSF405-400261 (239.00), OSF405-400302 (278.00), OSF405-400307 (282.00), OSF405-400331 (339.00), OSF405-400331-1 (339.01), OSF405-400323 (316.00), OSF405-400334 (321.00), OSF405-400341 (324.00), OSF405-400348 (329.00), OSF405-400372 (342.00), OSF405-400400 (355.00), OSF405-400402 (356.00), OSF405-400403 (362.00), OSF405-400408 (365.00), OSF405-400410 (372.00), OSF405-400417 (394.00), OSF405-400430 (413.00), OSF405-400448 (424.00), OSF405-400449 (425.00), OSF405-168 (476.00), OSF405-169 (479.00), OSF405-179 (487.00), OSF405-181 (494.00), OSF405-191 (498.00), OSF405-192 (501.00), OSF405-217 (519.00), OSF405-175 (499.00), OSF405-400203 (173.00), OSF405-400115 (100.00), OSF405-165 (475.00), OSF405-272 (624.00), OSF405-308 (654.00), OSF405-312 (657.00), OSF405-317 (661.00), OSF405-321 (663.00), OSF405-341 (680.00), OSF405-349 (686.00), OSF405-380 (716.00), OSF405-381 (717.00), OSF405-391 (727.00), OSF405-389 (725.00), OSF405-400118 (102.00), OSF405-400169 (133.00), OSF405-400234 (213.00), OSF405-400270 (261.00), OSF405-400304 (279.00), OSF405-400326 (319.00), OSF405-400435 (416.00), OSF405-301 (649.00), OSF405-331 (671.00), OSF405-400193 (166.00), OSF405-400434 (415.00), OSF405-343 (681.00), OSF405-159 (508.00), OSF405-365 (701.00), OSF405-400073 (73.00), OSF405-033 (33.00), OSF405-400122 (104.00), OSF405-400122B (304.00), OSF405-422 (751.00), OSF405-400079 (78.00), OSF405-400382 (391.00), OSF405-296 (644.00), OSF405-400437A (784.00), OSF405-520 (795.00) This patch corrects the following: • 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 with the DECthreads "legacy" library. • 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 to exception handling. • Threaded applications seeing a deadlock with fork(), premature stack overflows, corrupted mutexes, orphaned condition variable or mutex blocking structures. • Multi-threaded programs running on a multiprocessor may behave as if they have fewer CPUs available for execution. A considerable performance degradation can be observed in some cases.

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

Patch 737.00 continued	• 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 with the mkpasswd command. Hashed password database files (for example, /etc/passwd.pag and /etc/passwd.dir) are deleted before new database files are created. • Fixes a problem in which mallopt(M_MXFAST), instead of making malloc() faster makes it as much as 65 times slower. • 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. • Older call_shared FORTRAN applications to find missing symbols in libc.so. • 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 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. • 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. • A problem that prevents gethostent() from returning all YP or bind served entries.

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

Patch 737.00 continued	• inet_makeaddr() routine in libc that was returning 8 bytes instead of 4. • Deadlocks that may occur in multithreaded applications which make concurrent use of the fork() and fclose() functions, or the getenv()/setenv() and any time-related function (e.g., localtime()). • A problem from memory leaks with heavily threaded applications using NIS services for passwd, group, and other system database files. • The malloc function fails to allocate all available space within the 2GB address space allowed by the taso option. • This patch 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. 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.

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

Patch 737.00 continued	• 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 DIGITAL UNIX 4.0. An exception occurring 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 occasionally being lost. – Stack unwinding during exception processing was losing contexts, resulting in incorrect stack traces. • 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). • 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). • 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 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.

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

Patch 737.00 continued	• 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. • Fixes an AdvFS problem in which improper handling of I/O queues causes either a kernel memory fault or the following panics: "bs_invalidate: cache rundown" "rm_or_moveq: ioDesc not on a queue" • Command nslookup will sometimes display the incorrect error message for non-English locales. • 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 with the syslog function. Some syslog messages may fail to 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.

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

Patch 737.00 continued	• 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 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(). • 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. • 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. • 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.

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

Patch 737.00 continued	• Fixes a problem where 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 • Adds automatic detection of a cdfs file system for the mount(8) command.

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

Patch 737.00 continued	• 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 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 with the ksh shell program. ksh prevents a command which runs in a sub-process from writing to a tape device. • 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: /bin/ksh: invalid multibyte character • 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 Korn shell in which the "lt" operator did not 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 problems can cause the "grep" and "find" commands to fail, when the user runs 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.

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

Patch 737.00 continued	• Fixes the problem that csh may omit the data byte 0x80 when processing a a string in the ja_JP.SJIS or zh_TW.big5 locales. • 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 management problem that occurs on systems running the Korn shell. Incorrect results occur when the length of the parameter to the echo command is altered. • Corrects quota command to return worst error status on exit. • Allows system managers to both set and obtain quotas for users and groups which are numeric when using the edquota, vedquota, quota, and vquota programs. • 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 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. • 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". • 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 739.00 OSF405-406	**Patch:** Mail Corrections, Security (SSRT0421U) **State:** Supersedes patches OSF405-400063 (64.00), OSF405-400071 (71.00), OSF405-400071-1 (71.01), OSF405-400160-1 (128.01) This patch corrects the following: • A potential security vulnerability has been discovered in 'libXt', where under certain circumstances users may gain unauthorized access. DIGITAL has corrected this potential vulnerability. • If the user sending mail makes an error entering the destination address the user will receive a mail message that contains both the text of the mail and the error messages. The error messages do not correctly describe the exact nature of the problem. • Mail fails when a large distribution list is used. • 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.

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

Patch 740.00 OSF405-407A	**Patch:** setacl Correction **State:** New This patch corrects the problem with setacl not being able to handle a user ID beginning with a numeral.
Patch 741.00 OSF405-408	**Patch:** Fix for AdvFS and /etc/fdmns directory links **State:** New. Supersedes patch OSF405-320 (662.00) This patch fixes the following problems: • 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 742.00 OSF405-409	**Patch:** Compiler Correction **State:** New This patch 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.
Patch 743.00 OSF405-411A	**Patch:** clock_settime Correction Improvement for AdvFS **State:** Supersedes patch OSF405-400215-1 (189.01) This patch fixes the following problems: • Fixes a problems 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 744.00 OSF405-412	**Patch:** Simple Lock Time Limit Exceeded Panic **State:** Supersedes patch OSF405-400255 (233.00) This patch fixes the following problems: • 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 coalesced via physio while in read/writeback mode.

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

Patch 748.00 OSF405-418	**Patch:** dbx Correction **State:** Supersedes patches OSF405-400205 (177.00), OSF405-257 (611.00), OSF405-413 (745.00) This patch fixes the following: • 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.
Patch 749.00 OSF405-420	**Patch:** Add Support For DE500-BA 10/100 Ethernet Adapter Supersedes patches OSF405-400066 (67.00), OSF405-069B (238.00), OSF405-069 (221.00), OSF405-066 (208.00), OSF405-400218 (193.00), OSF405-097 (252.00), OSF405-108 (308.00), OSF405-376 (712.00) This patch corrects the following: • Boot capability for new hardware support requires a new genvmunix. This patch delivers an updated genvmunix for that purpose. • Add support for DE500-BA 10/100 Ethernet adapter, and fix machine checks encountered when using the KZPAM-CA or KZPAM-DA controllers. • This patch is an upgrade/replacement for the Ethernet driver when a DE500-AA Fast Ethernet interface is used. This driver, when used with a DE500-AA containing the DECchip 21140-AC, will allow filtering of greater than 16 multicast addresses and fixes the previous limitations to Hash/Perfect mode filtering. • DDR subsystem updated to handle SCSI devices returning a non-standard device type. • ddr_config would sometimes build partial device records. • ddr_config not compatible with input files created prior to this version. prior to this version. • Adds device recognition for TZS2. • This patch is an 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 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. • 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 759.00 OSF405-433	**Patch:** Interrupt Handling Correction **State:** Supersedes patch OSF405-246 (572.00) 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 760.00	**Patch:** Various Kernel Fixes, Security (SSRT0482U, SSRT0521U)
OSF405-434A	**State:** Supersedes patches OSF405-400082 (80.00), OSF405-400099 (90.00), OSF405-400110 (98.00), OSF405-400127 (107.00), OSF405-025 (25.00), OSF405-400054 (58.00), OSF405-400057 (60.00), OSF405-400100 (91.00), OSF405-400113 (99.00), OSF405-034 (34.00), OSF405-036 (36.00), OSF405-037 (37.00), OSF405-038 (38.00), OSF405-040 (40.00), OSF405-400141 (116.00), OSF405-400165 (129.00), OSF405-400197 (170.00), OSF405-058 (174.00), OSF405-054 (155.00), OSF405-400180 (160.00), OSF405-400200 (171.00), OSF405-400213 (186.00), OSF405-062 (195.00), OSF405-048 (48.00), OSF405-400104 (94.00), OSF405-045 (45.00), OSF405-068 (220.00), OSF405-400201 (172.00), OSF405-029 (29.00), OSF405-031 (31.00), OSF405-044 (44.00), OSF405-052 (52.00), OSF405-053 (53.00), OSF405-059 (187.00), OSF405-400186 (162.00), OSF405-071 (222.00), OSF405-400221 (197.00), OSF405-400208 (182.00), OSF405-400056 (59.00), OSF405-400198 (196.00), OSF405-400224 (200.00), OSF405-400216 (190.00), OSF405-400233 (212.00), OSF405-400232 (211.00), OSF405-400212 (185.00), OSF405-400235 (217.00), OSF405-400242 (224.00), OSF405-400250 (229.00), OSF405-400245 (226.00), OSF405-400266 (258.00), OSF405-400240 (231.00), OSF405-400289 (271.00), OSF405-400296 (276.00), OSF405-400298 (277.00), OSF405-067 (219.00), OSF405-400130 (109.00), OSF405-081 (242.00), OSF405-098 (253.00), OSF405-400351 (300.00), OSF405-102 (274.00), OSF405-400273 (262.00), OSF405-400281 (265.00), OSF405-400283 (267.00), OSF405-400316 (293.00), OSF405-400342 (325.00), OSF405-400346 (328.00), OSF405-400348 (329.00), OSF405-400353 (330.00), OSF405-400354 (331.00), OSF405-400356 (332.00), OSF405-400357 (333.00), OSF405-400360 (352.00), OSF405-400367 (376.00), OSF405-400369 (374.00), OSF405-400373 (360.00), OSF405-400378 (358.00), OSF405-400384 (375.00), OSF405-400284 (268.00), OSF405-400093 (87.00), OSF405-400393 (359.00), OSF405-400397 (366.00), OSF405-400401 (357.00), OSF405-400407 (363.00), OSF405-103 (290.00), OSF405-114 (303.00), OSF405-116 (312.00), OSF405-123 (369.00), OSF405-065 (207.00), OSF405-121 (380.00), OSF405-129 (382.00), OSF405-130 (383.00), OSF405-133 (463.00), OSF405-134 (386.00), OSF405-138 (387.00), OSF405-145 (460.00), OSF405-136 (379.00), OSF405-400414 (400.00), OSF405-400418 (403.00), OSF405-400420 (404.00), OSF405-400421 (405.00), OSF405-400441 (420.00), OSF405-400451 (427.00), OSF405-400442 (421.00), OSF405-400456 (430.00), OSF405-400461 (433.00), OSF405-400466 (438.00), OSF405-125 (370.00), OSF405-400469 (441.00), OSF405-400470 (465.00), OSF405-153 (477.00), OSF405-173 (486.00), OSF405-155 (488.00), OSF405-177 (489.00), OSF405-209 (509.00), OSF405-142 (513.00), OSF405-210 (515.00), OSF405-204 (518.00), OSF405-216 (521.00), OSF405-207 (524.00), OSF405-206 (525.00), OSF405-185 (533.00), OSF405-162 (534.00), OSF405-221 (536.00), OSF405-229 (541.00), OSF405-230 (542.00), OSF405-199 (546.00), OSF405-243 (548.00), OSF405-247 (550.00), OSF405-200 (551.00), OSF405-198 (562.00), OSF405-238 (563.00), OSF405-252 (571.00), OSF405-292 (580.00), OSF405-281 (581.00), OSF405-176 (514.00), OSF405-187 (492.00), OSF405-189 (604.00), OSF405-190 (605.00), OSF405-259 (613.00), OSF405-265 (618.00), OSF405-268 (621.00), OSF405-269 (622.00), OSF405-274 (626.00), OSF405-276 (628.00), OSF405-277 (629.00), OSF405-278 (630.00), OSF405-287 (637.00), OSF405-289 (638.00), OSF405-291 (640.00), OSF405-293 (641.00), OSF405-302 (650.00), OSF405-305 (652.00), OSF405-313 (658.00), OSF405-322 (664.00), OSF405-325 (666.00), OSF405-330 (670.00), OSF405-335 (674.00), OSF405-339 (678.00), OSF405-340 (679.00), OSF405-345 (683.00), OSF405-348

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

Patch 760.00 continued	(685.00), OSF405-352 (688.00), OSF405-354 (690.00), OSF405-355 (691.00), OSF405-356 (692.00), OSF405-357 (693.00), OSF405-362 (698.00), OSF405-364 (700.00), OSF405-366 (702.00), OSF405-367 (703.00), OSF405-368 (704.00), OSF405-371 (707.00), OSF405-378 (714.00), OSF405-379 (715.00), OSF405-383 (719.00), OSF405-384 (720.00), OSF405-392 (728.00), OSF405-393 (729.00), OSF405-394 (730.00), OSF405-397 (732.00), OSF405-404 (738.00), OSF405-421 (750.00), OSF405-429 (755.00), OSF405-430 (756.00), OSF405-431 (757.00), OSF405-435 (761.00), OSF405-149 (490.00), OSF405-223 (538.00), OSF405-448 (773.00), OSF405-267 (620.00), OSF405-350 (687.00), OSF405-299 (647.00), OSF405-307 (653.00), OSF405-388 (724.00), OSF405-414 (746.00), OSF405-426 (753.00), OSF405-363 (699.00), OSF405-439 (765.00), OSF405-441 (767.00), OSF405-443 (769.00), OSF405-450 (775.00), OSF405-442 (768.00), OSF405-445 (771.00), OSF405-328A (668.00) This patch corrects the following: • Fixes a problem in which network applications communicating to one 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. • 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.

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

Patch 760.00 continued	• Fixes a problem that occurs in the vm subsystem. The system panics with a "PANIC: VL_UNWIRE: PAGE IS NOT WIRED" message. This panic occurs most frequently on systems running database applications. • Fixes a performance problem that occurs with UFS file systems. • 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. • This patch corrects 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. • Fixes problems encountered when using signals with multithreaded programs. • 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. • When compiling a C++ program, an error message like the following is returned: cxx: Error: toto.cc, line 9: In this statement, "_Plocaltime_r" is not declared. The interface given in the error message will always begin with _P and end with _r. • Fixes a problem that occurs when the system panics with the following error message: Kernel memory fault • Fixes a problem in which the ufs property list can become corrupted. • 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. • Fixes a problem in which the system can panic with "lock already owned by thread".

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

Patch 760.00 continued	• 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. A representative console message indicating this condition are shown below: SIS00-00-root: IP q full, 315617 packets dropped in the last 5 mins. • Fixes ICMP REDIRECTS. When an ICMP REDIRECT is received, the routing table was updated properly, but the IP layer didn't use the new route information. • Fixes a problem that occurs on all systems that use networking services. • A kernel fix for network sockets left in FIN_WAIT_1 state forever. This patch contains a "tuneable" kernel parameter. It is recommended that only experienced system administrators attempt to set this parameter from the default value. This patch is MANDATORY to install. • A system panic caused by a Windows95 or WindowsNT system sending an illegal length ping (ICMP)packet. • A kernel memory fault panic that occurs in ip_forward. • Fixes a kernel memory fault in ether_output packet filter, when running tcpdump. • This patch does the following: – Fixes an isp1020 SCSI driver performance regression. – Provides HSZ70 support. • Probe of isp fails intermittently during boot. • Fixes a problem that occurs with the Qlogic driver. Because of a problem with the sim code, command timeouts occur and the printer device will not be detected during SCSI device configuration. • Fixes kernel asynchronous I/O (AIO) problems that occur on clustered systems and systems using major database products on raw disk partitions. Users of database products are advised to install this AIO patch. • The kernel panics with a "kernel memory fault", typically in either the vm_pg_alloc() or vm_zeroed_pg_alloc() routines. • This patch allows tuneability 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:" • 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 Version 4.2c requires this patch for new fcntl functionality. This layered product will not run desirably without this patch.

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

Patch 760.00 continued	• 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. • This patch resolves a kernel memory fault. • Fixes system crash when setting the date on SMP systems. • Fixes a network socket problem with select() missing state changes on clients from non-write to writable. • vmstat(1) command displays negative numbers when used with the '-P' option. It is dependent on how the system constructs various internal data structures. • 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. • Devices sometimes cannot be accessed by the system after getting selection timeouts. • Fixes several problems, including system hangs and crashes in cam that can occur when running HSZ40/50/70s. • Fixes a problem that causes the system to panic after creating a symbolic link to the root file system ('/') and accessing it like a normal file. For an AdvFS file system, the system will panic with the following error message: bs_bf_htop: invalid handle For other file systems, the system will panic with the following error message: vrele:bad ref count

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

Patch 760.00 continued	• Prevents a "kernel memory fault" in bread() during sync operations. • This patch prevents duplicate namecache entries on SMP systems. • Calls to flock() can hang a process on an SMP system if 2 or more processes are attempting to obtain and release an flock() on the same file. • 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. • System panics with message: "vm_map_swapout: negative resident count". • Fixes a problem in which processes can hang waiting for a system call to table() to complete. • Fixes a problem that occurs when FORTRAN programs or multithreaded applications that were built on a V3.2C system are run on a DIGITAL UNIX V4.0A system. The system displays the following error message: "msg_copyout: map entry limit reached" • Corrects a problem in which the system will panic with "u_shm_oop_deallocate: reference count mismatch." • 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 improvement. • 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 760.00 continued	• Fixes a problem with the "ifconfig -a" command. At times, the command will not display all of the network interfaces. • Adds a mechanism to the poll() system call to allow it to be used as a timer. • Provides additional event logging by the SCSI/CAM disk driver to the binary.errlog file. • Fixes a panic 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. • Fixes a problem that occurs when using real-time applications. When writing large (sequential) files to a UFS file system, time constraints associated with the application may be violated. • Eliminates panics that will occur when attempting to execute shell scripts on a filesystem mounted with the "noexec" option. • 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 • Fixes a problem in which a system hang or core dump occurs when one program inadvertently overwrites the contents of another program.

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

Patch 760.00 continued	• System experiences simple lock timeout panics in virtual memory routines when free memory is short and system is trying to reclaim memory. • A potential security vulnerability has been discovered, where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability. • Fixes several problems in the vm subsystem: – Processes using shared memory (SSM) may hang. – Skewed swap space is not allocated evenly. – shmget() failure can cause "Machine Check 660." • 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 the correct values for each individual fileset. • 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 problems in the mkpasswd command. • 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 SMP systems with AdvFS file systems. Fixes a performance degradation problem that may occur. • Fixes a problem that may occur after a system panics. The system may hang when trying to do a crash dump.

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

Patch 760.00 continued	• This is a mandatory patch for AlphaServer 2000 and AlphaServer 2100 SMP systems. This patch fixes the following problems: – Internal lockups may cause performance degradation. – The system clock may lose time. • 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 • This patch contains two vm fixes in both the UFS and NFS code that collectively resolve a multitude of nfs and nfsd hangs. • Fixes a problem that causes some valid programs compiled with IEEE mode to receive a floating-point exception even though they should run to completion. • 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. • Fixes a problem that may cause a program to cause the IEEE floating point emulator to emit this message: "FATAL IEEE FLOATING POINT EMULATION ERROR:" • 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. • Back-port of PTMIN-style multioption 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.

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

Patch 760.00 continued	• Resolves an inode locking problem in the UFS iupdat() and itimes functions. • Fixes a problem in which a system may crash if multiple bad blocks on a SCSI device are encountered simultaneously. • Provides the following support: – Support the HSZ70 Raid controller on the Fast10 Wide Differential KZPSA adapter in cluster environments under DIGITAL UNIX V4.0A. Support of the HSZ70 Raid controller also requires the KZPSA firmware to be upgraded to at least the version distributed on the Version 5.0 AlphaServer Console Firmware CDrom. – Performance regression fix for Qlogic isp1020/isp1040 chips. – Provide SCSI target mode fixes for ASE/TCR support on QLogic, primarily for HSZ70 support. – All modifications included in this patch are compatible with existing versions of KZPSA and Qlogic firmware. • 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. • 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. • Infrequently, under heavy disk I/O loads, user data can be written to the wrong disk, resulting in data corruption. • Provides Qlogic sim driver support for the HSZ70 and HSZ50 Raid controllers in cluster environments running ASE/TCR 1.4A on the KZPBA-CB wide differential UltraSCSI adapter. Complete support for cluster environments also requires that the Qlogic adapter firmware version is at least at the level as in the HSZ70 Raid Controller Platform Kit. • Fixes a problem in which a file-on-file system mount of either an NFS or a /proc file system will panic the system. • Fixes two kernel memory faults in networking code.

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

Patch 760.00 continued	• This patch corrects problems with AdvFS performance regression, and two AdvFS race condition situations between multiple routines that can cause panics. • 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 • 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 • Fixes a problem that causes the system to panic with the following error message: u_anon_free: page busy • Provides two new procfs ioctls (PIOCUSAGE and PIOCTUSAGE) to collect task and thread wait time statistics. • 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 V4.0A, in conjunction with Version A11 KZPSA firmware or greater. • 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

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

Patch 760.00 continued	• 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 core() system call would try to dump from a memory region that has no permission, causes an access violation in core() and the core file would |be unusable. An example of the problem: % file core core: core dump, core file is incomplete % dbx program core . . . can't attach to loader: I/O error Exiting due to error during startup • Fixes a problem with the ufs_fsck. ufs_fsck would mishandle certain dir corruptions, recursively asking the user if they want to fix it. • Fixes a problem of memory corruption. A TCP control structure is illegally accessed after it is released. The corrupted memory buckets are the 256-byte size. • Fixes a problem in which the uswitch system call does not work when an application tries to reset the USW_NULLP option. • 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 panic that occurs when the system's message buffer size is increased to beyond the default size of 4096. During the subsequent reboot, the syslogd daemon fails with a "Segmentation fault (core dumped)" message, and creates a core file in the "/" directory.

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

Patch 760.00 continued	• Fixes a race condition whereby the pid_block() system call does not properly synchronize with signals. This problem could cause the system call to block and not take a signal when it is supposed to. • Provides a set of workarounds for Qlogic firmware bugs. These bugs were encountered when using the HSZ70 Raid Array Controller on the KZPBA-CB wide differential UltraSCSI adapter in a dual-node cluster environment. • 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: "ialloc: dup alloc" • Improves performance on low-memory (32MB) systems. • Extends the KMEM_DEBUG_PROTECT option of kmem_debug to the 8192-byte bucket. • Fixes a problem that occurs on SMP systems. The system panics with the following message: kernel lock violation: thread_lock • Fixes a problem in which the system may panic with the following message: simple_lock: lock already owned by cpu • 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. • 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 kernel memory fault panic in purge_fs_locks. This problem is normally only seen on ASE or TruCluster systems. • 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 problem with the ufs_fsck program in which filesystem corruption may occur on a running system when the root filesystem is mounted writable. • 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. • Prevents a "kernel memory fault" in the bread() routine while performing sync operations. • Fixes a kernel memory fault in the networking code.

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

Patch 760.00 continued	• Fixes a panic in the virtual memory management system. The system displays the following error message: trap: invalid memory read access from kernel mode • Corrects a synchronization problem by blocking out hardclock before touching the state visible to the clock interrupt routine. • Fixes a problem that produces a core dump when running the quotacheck -a command. The following panic string is displayed: Segmentation fault at strcmp • 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. • Corrects a problem in how the ps command reports its accumulated CPU time of all exited threads. • Corrects a problem where the NXM_IEEE_STATE_COPYIN/OUT macros need to save/restore the pcb nofault state. This was not happening. • 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. • Fixes a kernel memory fault panic. This patch is mandatory for all all multiprocessor machines. • Fixes a "mount device busy" problem that occurs when a user cannot overwrite the file "core". This prevents the filesystem from being umount'ed. • 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 panic with the following error message: trap: invalid memory write access from kernel mode • Corrects a problem in memory allocation where a tasks resident count could become inconsistent, causing a panic. • Corrects a problem where process hangs are caused by file references on raw devices accesses not being held. • Fixes 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. • Fixes the problem in which a DIGITAL UNIX system can randomly panic when more than 255 network interfaces are configured. • Corrects a problem where a flag, TF_PSUSP, was not being cleared. • Fixes a problem that produced a deadlock between process threads. Typically, the deadlock caused the msfs_getpage routine to wait forever for a lock to be released.

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

Patch 760.00 continued	• Fixes a problem when a processor is commanded to stop during a heavy load but does not actually halt. • Corrects a problem that causes a "pmap_ssm_destroy: wired pages" crash. • Corrects a performance 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. • Corrects a problem seen with DECthreads tests that use fork(2). • In some instances, a message size of zero passed to msgsnd() can result in a kernel memory fault panic. • 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. • 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.

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

Patch 760.00 continued	• 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 problem that would randomly cause kloadsrv(8) to crash and improperly load/unload modules. • 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. • Corrects a simple lock timeout problem in several vm_page routines. • Changed 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 two Kernel Memory Faults in DIGITAL UNIX Path MTU discovery code. • Fixes a TCP/IP performance problem in the tcp_reass() function. • Removes extraneous debug code. • Fixes a problem in which the system can panic with the message "kernel memory fault". • Fixes a system panic "rtfree 2" on multi-cpu systems. • 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.

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

Patch 760.00 continued	• Prevents a kernel malloc leak when changing the protection of a System V shared memory region that uses gh-chunks. • 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 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 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.

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

Patch 760.00 continued	• 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 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". • Fixes a problem in the kernel that caused dynamically loaded PCI/ISA drivers to crash the system with the following panic: 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. • 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 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 when a setuid program is exec'ed, and the error message "privileges disabled because of outstanding IPC access to task" is issued. • 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. • Fixes an ASE NFS problem that occurs on ASE systems with KZPBA disk controllers. The system crashes with a "simple_lock timeout" panic. • Prevents a system panic from m_copym(). • 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.

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

Patch 760.00 continued	• Fixes a problem with the vmstat -P command, which was incorrectly formatting output. • Fixes a problem with user stack pointers not being saved properly in kernel crash dumps for running threads. • 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 • 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 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 a problem in which 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. • Fixes a problem with the KZPSA and KZTSA SCSI adapters. The adapters will hang if the SCSI cable is disconnected from them. • Fixes a kernel memory fault in cansignal(). • 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. • Corrects a small accounting problem where the measured time for a process was an integral rather than mean value. • Fixes the following problems in AdvFS: – An 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.

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

Patch 762.00 OSF405-436	**Patch:** Security, (SSRT0476U) **State:** Supersedes patches OSF405-023 (23.00), OSF405-400146 (119.00), OSF405-400236 (218.00), OSF405-400324 (317.00), OSF405-400368 (340.00), OSF405-184 (559.00), OSF405-051 (51.00), OSF405-100 (255.00), OSF405-143 (464.00), OSF405-028 (28.00), OSF405-080 (241.00), OSF405-128 (385.00), OSF405-202 (555.00), OSF405-423 (752.00), OSF405-432 (758.00) 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. • System panics with a kernel memory fault or "malloc_audit: guard space corruption" with osr_run as an entry in the stack. • This patch 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. • Fixes a problem that occurs on a system when running STREAMS. The system panics with the following error message: "kernel memory fault" • The ASDU netbeui server (nbelink) will not close a connection. It will hang in dlcb_close awaiting a STREAMS event. Subsequently, new connections will not be able to connect to nbelink. • The STREAMS tty line discipline not correctly processing type ahead characters. Also this patch fixes a delay in closing the STREAMS tty line discipline (typically seen on LAT connections). • Fixes a wide variety of system panics and other problems caused by random memory corruption. • Fixes a problem when printing to slow printers using DIGITAL UNIX LAT. The end of a large file fails to print and no error is reported. • Allows user control messages to be passed between a STREAMS pty pair. This capability was not available in the original released software. • 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.

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

Patch 762.00 continued	• Fixes a problem in which the system panics with one of the following error messages: simple_lock: uninitialized lock simple_lock_terminate: lock busy • Fixes a problem in which the system may panic with the following error message "kernel memory fault".
Patch 766.00 OSF405-440A	**Patch:** Greater Than 500 XTI Connections Crash Correction **State:** Supersedes patches OSF405-400171 (135.00), OSF405-400196 (169.00), OSF405-400264 (257.00), OSF405-400385 (395.00), OSF405-400151 (123.00), OSF405-400405-1 (397.01), OSF405-237 (607.00) This patch corrects the following: • 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. • Fix for a mutex lock problem in TLI. The problem causes multithreaded TLI applications to block forever. • 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. • This patch fixes a problem that occurs on a system when running STREAMS. The system panics with the following error message: kernel memory fault • Fix to libtli/libxti to correctly handle a continuation data message still on the stream head.
Patch 772.00 OSF405-447	**Patch:** Kernel Build config Command Correction **State:** New This patch fixes a problem in which the kernel build config command (obj/alpha/kernel/bin/config) core dumps if the fopen function fails.
Patch 774.00 OSF405-449	**Patch:** Rsh and sh Command Corrections **State:** Supersedes patch OSF405-400069-1 (69.01) This patch corrects the following problems that occur when an application is started from a subshell, for example, sh -c <command>. • An application will hang if it receives an interrupt signal, for example, if the user enters Ctrl/C. • While an application is running, if Ctrl/C is entered, the parent process exits, but the child process remains. • 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).

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

Patch 776.00 OSF405-451	**Patch:** Audit Record Correction **State:** New This patch fixes a problem in which audit records are generated for selected operations against objects that are not in the filesystem.
Patch 777.00 OSF405-453A	**Patch:** Curses Library Correction **State:** New This patch 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 778.00 OSF405-454	**Patch:** Dynamically Configured Device Drivers On An EISA Bus **State:** Supersedes patch OSF405-400170 (134.00) 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 781.00 OSF405X11-011A	**Patch:** xterm Correction, Security (SSRT0422U, SSRT0547U) **State:** Supersedes patches OSF405X11-400010 (152.00), OSF405X11-400017 (289.00), OSF405X11-400021 (367.00) 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.

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

Patch 783.00 OSF405X11-013	**Patch:** Screen Flickers In Power_Save Mode Correction **State:** Supersedes patches OSF405X11-400013 (214.00), OSF405X11-400014 (215.00), OSF405X11-012 (782.00) This patch corrects the following: • On systems with PowerStorm 4D40T, 4D50T, or 4D60T graphics options, the X server may hang every 49 days. • 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. • This patch 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 785.00 OSF405CDE-008B	**Patch:** dtterm Corrections **State:** Supersedes patches OSF405CDE-400003 (138.00), OSF405CDE-400004 (139.00), OSF405CDE-400012 (453.00), OSF405CDE-400014-1 (455.01) 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. • Prevents the escape sequence that sets DECterm window titles from hanging dtterm windows. • 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 786.00 OSF405-328B	**Patch:** acctcom Command Correction **State:** Supersedes patch OSF405-400230 (209.00) This patch fixes the following problems: • 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 788.00 OSF405-407B	**Patch:** setacl Development Correction **State:** New This patch 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 789.00 OSF405-411B	**Patch:** Performance Improvement for AdvFS **State:** Supersedes patches OSF405-400215 (189.00), OSF405-400215B (587.00) This patch fixes the following problems: • Fixes a problems 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 791.00 OSF405-453B	**Patch:** Curses Library Development Correction **State:** New This patch 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 792.00 OSF405X11-011B	**Patch:** xterm LIBA Correction, Sec. (SSRT0422U, SSRT0547U) **State:** Supersedes patches OSF405X11-400010 (152.00), OSF405X11-400017 (289.00), OSF405X11-400021 (367.00) 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 793.00 OSF405X11-011C	**Patch:** xterm DEV Correction, Sec. (SSRT0422U, 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.

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

Patch 796.00 OSF405-440B	**Patch:** XTI libxti Library Correction **State:** Supersedes patches OSF405-400171 (135.00), OSF405-400196 (169.00), OSF405-400264 (257.00), OSF405-400385 (395.00), OSF405-400151 (123.00), OSF405-400405 (397.00), OSF405-400405B (586.00) This patch corrects the following: • 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. • Fix for a mutex lock problem in TLI. The problem causes multithreaded TLI applications to block forever. • 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. • Fix to libtli/libxti to correctly handle a continuation data message still on the stream head.

Patch 798.00
OSF405-403B
	Patch: named Command Correction, (SSRT0296U, SSRT0494U)
	State: Supersedes patches OSF405-400189 (164.00), OSF405-400189B (246.00), OSF405-400189B-1 (246.01), OSF405-400313 (283.00), OSF405-400422 (406.00)
	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.
	• Corrects a problem where, if the FLAG bit is set in the IP header, screend incorrectly reports:
	`ACCEPT: Not first frag, off 64`
	• 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 an AdvFS filesystem. The panic has following stack trace:
	`panic (s = "spec_badop called")`
	`spec_badop`
	`fpathconf`
	`syscall`
	`_Xsyscall`
	• 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.

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

Patch 801.00 OSF405CDE-400006A	**Patch:** Nodename Length Correction CDE Environment **State:** Supersedes patch OSF405CDE-400006 (154.00) 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 802.00 OSF405CDE-400006B	**Patch:** Nodename Length Correction **State:** Supersedes patch OSF405CDE-400006 (154.00) 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 803.00 OSF405-400331C-2	**Patch:** lprsetup Command Correction **State:** Supersedes patches OSF405-400331 (339.00), OSF405-400331C-1 (302.01) 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.
Patch 804.00 OSF405-400331C-3	**Patch:** OSF405-400331C-3 **State:** Supersedes patches OSF405-400331 (339.00), OSF405-400331C-1 (302.01) 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.
Patch 805.00 OSF405-248A	**Patch:** Run-Time Support For DIGITAL C++ V6.0 Compiler **State:** Supersedes patches OSF405-400487 (452.00), OSF405-248 (545.00) This patch corrects the following: • Provides 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. • An updated libcxx.so which provides the required run-time support for images created by DIGITAL C++ V6.0 and above. Customers who are using DIGITAL C++ V6.0 can use the un-documented compiler switch: -use_system_libcxx which will cause the compiler to use the system libcxx.so file when linking. DIGITAL C++ V6.0 customers should only use this switch if the resulting images are to be executed either on other systems witch have had the libcxx.so patch installed, or on DIGITAL UNIX V4.0D and above systems.

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

Patch 806.00 OSF405-248B	**Patch:** Support For DIGITAL C++ V6.0 Compiler (static) **State:** Supersedes patches OSF405-400487 (452.00), OSF405-248 (545.00) This patch corrects the following: • Provides 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. • An updated libcxx.so which provides the required run-time support for images created by DIGITAL C++ V6.0 and above. Customers who are using DIGITAL C++ V6.0 can use the un-documented compiler switch: -use_system_libcxx which will cause the compiler to use the system libcxx.so file when linking. DIGITAL C++ V6.0 customers should only use this switch if the resulting images are to be executed either on other systems witch have had the libcxx.so patch installed, or on DIGITAL UNIX V4.0D and above systems.
Patch 807.00 OSF405X11-400019A	**Patch:** DECwindows Motif toolkit **State:** Supersedes patch OSF405X11-400019 (348.00) This patch 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 808.00 OSF405X11-400019B	**Patch:** Motif toolkit **State:** Supersedes patch OSF405X11-400019 (348.00) This patch 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 809.00 OSF405X11-010A	**Patch:** Motif Toolkit Correction Patch **State:** Supersedes patches OSF405X11-400015 (216.00) OSF405X11-400020 (349.00), OSF405X11-009 (577.00), OSF405X11-010 (780.00) 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 810.00 OSF405X11-010B	**Patch:** Motif Toolkit Correction **State:** Supersedes patches OSF405X11-400015 (216.00) OSF405X11-400020 (349.00), OSF405X11-009 (577.00), OSF405X11-010 (780.00) 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.
Patch 811.00 OSF405X11-007A	**Patch:** dtterm Displays All Characters in PC Codeset IBM-850 **State:** Supersedes patches OSF405-400468 (440.00), OSF405X11-007-1 (390.01) This patch corrects the following: • Provides the ability to let dtterm display all the characters in the PC codeset IBM-850. • Provides a new en_US.cp850 locale for processing text data originating from the PC environment.
Patch 812.00 OSF405X11-007B	**Patch:** dtterm Displays All Characters in IBM-850 PC Codeset **State:** Supersedes patches OSF405-400468 (440.00), OSF405X11-007-1 (390.01) This patch corrects the following: • Provides the ability to let dtterm display all the characters in the PC codeset IBM-850. • Provides a new en_US.cp850 locale for processing text data originating from the PC environment.
Patch 813.00 OSF405-279A	**Patch:**ftp Command Corrections, (SSRT0505U) **State:** Supersedes patches OSF405-400396 (393.00), OSF405-400144 (118.00), OSF405-400150 (122.00), OSF405-400396-1 (393.01), OSF405-161 (482.00), OSF405-188 (495.00), OSF405-279 (631.00) 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. • Fixes a problem where telnet dumps core if the USER environment variable is the last variable in the environment list. • Corrects a problem with rsh(1) that is most visible with long-distance (slow) links where a packet might get dropped.

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

Patch 814.00	**Patch:** yppush Command Corrections, (SSRT0505U)
OSF405-279B	**State:** Supersedes patches OSF405-400396 (393.00), OSF405-400144 (118.00), OSF405-400150 (122.00), OSF405-400396-1 (393.01), OSF405-161 (482.00), OSF405-188 (495.00), OSF405-279 (631.00) 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. • Fixes a problem where telnet dumps core if the USER environment variable is the last variable in the environment list. • Corrects a problem with rsh(1) that is most visible with long-distance (slow) links where a packet might get dropped.

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

Patch 815.00 OSF405-294A	**Patch:** LAN Emulation Conformance Correction Patch **State:** Supersedes patches OSF405-400072 (72.00), OSF405-400059 (62.00), OSF405-400078 (77.00), OSF405-400084 (82.00), OSF405-400102 (93.00), OSF405-400138 (113.00), OSF405-400219 (194.00), OSF405-400253 (232.00), OSF405-400286 (269.00), OSF405-400288 (270.00), OSF405-400411 (398.00), OSF405-400425 (408.00), OSF405-400432 (414.00), OSF405-400464 (436.00), OSF405-158 (480.00), OSF405-183 (507.00), OSF405-163 (510.00), OSF405-225 (532.00), OSF405-164 (537.00), OSF405-234 (560.00), OSF405-174 (493.00), OSF405-220 (523.00), OSF405-261 (614.00), OSF405-294 (642.00) 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). • Two panics in the lta driver, ATM LANE interoperability problems with IBM switches and slow recovery of UNI 3.0 signalling from network interruptions. • The system fails to establish one of the required VCs when joining an ATM Emulated LAN (LANE). • Fixes a number of kernel memory fault panics in the ATM subsystem. The panics are seen when the connection to the ATM switch is lost, particularly under heavy load. The patch also fixes problems with ATM timers and memory leaks. • Fixes a panic when the ATM driver is brought up/down and Lan Emulation (LANE) is active. A lockmode=4 (lock debug mode) panic is also fixed. • A problem with the ATM LAN Emulation code which was preventing correct emulation of Ethernet Multicast functionality. • A panic and other problems that can occur in the ATM subsystem when there is a large amount of signalling activity. It also fixes a potentially invalid signalling message. • 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. • Contains performance enhancements to the ATM OTTO driver when greater than 300 VC's are configured. This replacement driver uses hash buckets to improve search time in the VC data structure resulting in significant performance gains. • When tcpdump is run with ATM LAN emulation, a kernel memory fault occurs.

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

Patch 815.00 continued	• When tcpdump is run with ATM LAN emulation, a kernel memory fault occurs. • 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 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() • Upgrade enhancement to the ATM350 driver. This patch prevents panics in driver routines that can be called from different interrupt levels. • 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 panic from the ATM OTTO/OPPO driver. • Fixes two kernel memory faults and a system startup crash caused by the ATM convergence subsystem. • 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.

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

Patch 815.00 continued	• 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 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 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 816.00 OSF405-294B	**Patch:** LAN Emulation Conformance Correction **State:** Supersedes patches OSF405-400072 (72.00), OSF405-400059 (62.00), OSF405-400078 (77.00), OSF405-400084 (82.00), OSF405-400102 (93.00), OSF405-400138 (113.00), OSF405-400219 (194.00), OSF405-400253 (232.00), OSF405-400286 (269.00), OSF405-400288 (270.00), OSF405-400411 (398.00), OSF405-400425 (408.00), OSF405-400432 (414.00), OSF405-400464 (436.00), OSF405-158 (480.00), OSF405-183 (507.00), OSF405-163 (510.00), OSF405-225 (532.00), OSF405-164 (537.00), OSF405-234 (560.00), OSF405-174 (493.00), OSF405-220 (523.00), OSF405-261 (614.00), OSF405-294 (642.00) 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). • Two panics in the lta driver, ATM LANE interoperability problems with IBM switches and slow recovery of UNI 3.0 signalling from network interruptions. • The system fails to establish one of the required VCs when joining an ATM Emulated LAN (LANE). • Fixes a number of kernel memory fault panics in the ATM subsystem. The panics are seen when the connection to the ATM switch is lost, particularly under heavy load. The patch also fixes problems with ATM timers and memory leaks. • Fixes a panic when the ATM driver is brought up/down and Lan Emulation (LANE) is active. A lockmode=4 (lock debug mode) panic is also fixed. • A problem with the ATM LAN Emulation code which was preventing correct emulation of Ethernet Multicast functionality. • A panic and other problems that can occur in the ATM subsystem when there is a large amount of signalling activity. It also fixes a potentially invalid signalling message. • 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. • Contains performance enhancements to the ATM OTTO driver when greater than 300 VC's are configured. This replacement driver uses hash buckets to improve search time in the VC data structure resulting in significant performance gains. • When tcpdump is run with ATM LAN emulation, a kernel memory fault occurs.

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

Patch 816.00 continued	• When tcpdump is run with ATM LAN emulation, a kernel memory fault occurs. • 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 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() • Upgrade enhancement to the ATM350 driver. This patch prevents panics in driver routines that can be called from different interrupt levels. • 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 panic from the ATM OTTO/OPPO driver. • Fixes two kernel memory faults and a system startup crash caused by the ATM convergence subsystem. • 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.

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

Patch 816.00 continued	• 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 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 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 817.00 OSF405-400437A-1	**Patch:** lockinfo.c Correction **State:** Supersedes patches OSF405-032 (32.00), OSF405-400105 (95.00), OSF405-400148 (120.00), OSF405-400125 (105.00), OSF405-054 (155.00), OSF405-400176 (157.00), OSF405-400176-1 (157.01), OSF405-400217 (192.00), OSF405-400228 (206.00), OSF405-400239B (240.00), OSF405-400231 (210.00), OSF405-400259 (236.00), OSF405-094 (250.00), OSF405-400122 (104.00), OSF405-096 (251.00), OSF405-400315 (292.00), OSF405-400344 (327.00), OSF405-107 (307.00), OSF405-11 (310.00), OSF405-120 (371.00), OSF405-131 (388.00), OSF405-132 (462.00), OSF405-146 (461.00), OSF405-400389 (392.00), OSF405-400445 (423.00), OSF405-400474 (444.00), OSF405-400476 (445.00), OSF405-400489 (472.00), OSF405-400443 (422.00), OSF405-400497 (578.00), OSF405-241 (569.00), OSF405-400482 (450.00), OSF405-400482-1 (450.01), OSF405-170 (483.00), OSF405-171 (491.00), OSF405-156 496.00), OSF405-148 (505.00), OSF405-214 (522.00), OSF405-226 (528.00), OSF405-219 (530.00), OSF405-205 (531.00), OSF405-231 (535.00), OSF405-172 (539.00), OSF405-232 (540.00), OSF405-240 (543.00), OSF405-235 (544.00), OSF405-242 (549.00), OSF405-215 (558.00), OSF405-239 (565.00), OSF405-253 (568.00), OSF405-241 (569.00), OSF405-228 (570.00), OSF405-245 (553.00), OSF405-249 (608.00), OSF405-251 (610.00), OSF405-275 (627.00), OSF405-280 (632.00), OSF405-283 (634.00), OSF405-284 (635.00), OSF405-286 (636.00), OSF405-298 (646.00), OSF405-310 (655.00), OSF405-323 (665.00), OSF405-334 (673.00), OSF405-344 (682.00), OSF405-385 (721.00), OSF405-398 (733.00), OSF405-400 (734.00), OSF405-415 (747.00), OSF405-427 (754.00), OSF405-438 (764.00), OSF405-444 (770.00), OSF405-467 (779.00), OSF405-437 (763.00), OSF405-203 (506.00), OSF405-250 (609.00), OSF405-282B (787.00), OSF405-332 (672.00), OSF405-386 (722.00), OSF405-434B (790.00), OSF405-400437B (794.00) This patch corrects the following: • Fixes two problems that occur on AdvFS systems: – 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 817.00 continued	• NetWorker Version 4.2c requires this patch for new fcntl functionality. This layered product will not run desirably without this patch. • Fixes an AdvFS hang that could occur while running vdump. • Fixes an "ADVFS EXCEPTION, Module = 26" panic that occurs after an "advfs I/O error" console message. • Fixes a system panic with the message "simple_lock: time limit exceeded". • Fixes a problem where AdvFS hangs in routine cleanup_closed_list. • Fixes a problem that occurs on AdvFS systems. When a user exceeds the quota limits, an excessive number of user warning messages are sent to the system console if the user 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. • 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. • 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 problem that occurs on AdvFS systems. The system will panic with an error message similar to the following: panic (cpu 0): kernel memory fault

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

Patch 817.00 continued	• 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 (ACLs) 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 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 • Fixes two problems that occur on AdvFS systems: – The system may panic with the following error message: simple_lock: hierarchy violation – A locking problem in the AdvFS log data structures may cause the following problems to occur: ☐ System panics ☐ Kernel memory faults ☐ Memory corruption • Corrects a problem in AdvFS where a data structure fieldS is not initialized until after an AdvFS mount which is too late. This results in the inability for example to see the files after a remount. • Fixes an AdvFS problem in which the "advfsstat -n" command causes a core dump. The system displays the following error message: Memory fault(coredump) • Fixes a problem that occurs on AdvFS systems. If the "ls -l MI" command is given in a .tags directory, the fileset will become unmountable. If the system is then halted, a panic will occur.

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

Patch 817.00 continued	• Corrects a problem in AdvFS where a data structure field is not initialized until after an AdvFS mount which is too late. This results in the inability for example to see the files after a remount. • 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 of the following commands: # shutdown now # init s when AdvFS is the root or usr filesystem. • 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: 0xfffffc00006cad90 = "kernel memory fault" • Adds features and corrections to the AdvFS verify utility. • Fixes a problem that occurs on AdvFS systems. The chfsets function returns incorrect exit values and inappropriate error messages.

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

Patch 817.00 continued	• 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 problem that causes a lockmode 4 system panic. • 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 • 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 problem that occurs on AdvFS file systems. A kernel memory fault occurs on the AdvFS file system when accessing nfs-mounted files. • 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 situation where a quotacheck can cause a system panic. • Fixes a problem in which vrestore can cause an occasional core dump (Floating Exception). • 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.

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

Patch 817.00 continued	• Fixes AdvFS performance problems. • Fixes an kernel memory fault panic. The system displays the following error message: trap: invalid memory read access from kernel mode • This patch 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 • Corrects a problem where the mcellCount on-disk was not being updated as files were being migrated and this resulted in a panic situation. • This patch fixes a problem caused by the vrestore command. The command would fail when restoring multiple savesets from a TZS20 tape drive. • Provides a performance improvement for AdvFS systems. • 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 occurred when an AdvFS panic crashed the customer's system but the visible symptom was a crash due to a kernel memory fault. • Adds features and corrections to the AdvFS verify utility. The verify utility now detects and reports some file system corruption problems it had previously ignored. It also no longer gives seek errors on really large frag files (>2GB); gives detailed warning messages when a frag file is found to be incorrectly terminated, helping the user to know which file's fragments are involved; gives a useful error message when the root_domain is mounted read-only, preventing it from investigating other domains; properly handles domains that have clones; and properly handles SBM fixups (code which was intended to correct corrupted pages in the SBM metadata file fixed the page in memory but then wrote the newly corrected page over the NEXT page in the SBM.) Also, increases the amount of memory available to the program so that large memory systems can be worked with.

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

Patch 817.00 continued	• Corrects a panic and hang situation due to a limit of advfs access structures. • 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. • 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 message: 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.

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

Patch 817.00 continued	• 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 • 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 AdvFS that was causing a memory leak. • 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.

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

Patch 817.00 continued	• 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 with AdvFS that caused a page fault and the following panic: panic (cpu 0): kernel memory fault • 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 the AdvFS logging code, The way locking was implemented was causing degraded performance. • 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 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 818.00	**Patch:** Consolidated AdvFS Patches
OSF405-400437C	**State:** Supersedes patches OSF405-032 (32.00), OSF405-400105 (95.00), OSF405-400148 (120.00), OSF405-400125 (105.00), OSF405-054 (155.00), OSF405-400176 (157.00), OSF405-400176-1 (157.01), OSF405-400217 (192.00), OSF405-400228 (206.00), OSF405-400239B (240.00), OSF405-400231 (210.00), OSF405-400259 (236.00), OSF405-094 (250.00), OSF405-400122 (104.00), OSF405-096 (251.00), OSF405-400315 (292.00), OSF405-400344 (327.00), OSF405-107 (307.00), OSF405-11 (310.00), OSF405-120 (371.00), OSF405-131 (388.00), OSF405-132 (462.00), OSF405-146 (461.00), OSF405-400389 (392.00), OSF405-400445 (423.00), OSF405-400474 (444.00), OSF405-400476 (445.00), OSF405-400489 (472.00), OSF405-400443 (422.00), OSF405-400497 (578.00), OSF405-241 (569.00), OSF405-400482 (450.00), OSF405-400482-1 (450.01), OSF405-170 (483.00), OSF405-171 (491.00), OSF405-156 496.00), OSF405-148 (505.00), OSF405-214 (522.00), OSF405-226 (528.00), OSF405-219 (530.00), OSF405-205 (531.00), OSF405-231 (535.00), OSF405-172 (539.00), OSF405-232 (540.00), OSF405-240 (543.00), OSF405-235 (544.00), OSF405-242 (549.00), OSF405-215 (558.00), OSF405-239 (565.00), OSF405-253 (568.00), OSF405-241 (569.00), OSF405-228 (570.00), OSF405-245 (553.00), OSF405-249 (608.00), OSF405-251 (610.00), OSF405-275 (627.00), OSF405-280 (632.00), OSF405-283 (634.00), OSF405-284 (635.00), OSF405-286 (636.00), OSF405-298 (646.00), OSF405-310 (655.00), OSF405-323 (665.00), OSF405-334 (673.00), OSF405-344 (682.00), OSF405-385 (721.00), OSF405-398 (733.00), OSF405-400 (734.00), OSF405-415 (747.00), OSF405-427 (754.00), OSF405-438 (764.00), OSF405-444 (770.00), OSF405-467 (779.00), OSF405-437 (763.00), OSF405-203 (506.00), OSF405-250 (609.00), OSF405-282B (787.00), OSF405-332 (672.00), OSF405-386 (722.00), OSF405-434B (790.00), OSF405-400437B (794.00) This patch corrects the following: • Fixes two problems that occur on AdvFS systems: – 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 818.00 continued	• NetWorker Version4.2c requires this patch for new fcntl functionality. This layered product will not run desirably without this patch. • Fixes an AdvFS hang that could occur while running vdump. • Fixes an "ADVFS EXCEPTION, Module = 26" panic that occurs after an "advfs I/O error" console message. • Fixes a system panic with the message "simple_lock: time limit exceeded". • Fixes a problem where AdvFS hangs in routine cleanup_closed_list. • Fixes a problem that occurs on AdvFS systems. When a user exceeds the quota limits, an excessive number of user warning messages are sent to the system console if the user 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. • 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 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 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 • Fixes two problems that occur on AdvFS systems: – The system may panic with the following error message: simple_lock: hierarchy violation – A locking problem in the AdvFS log data structures may cause the following problems to occur: ☐ System panics ☐ Kernel memory faults ☐ Memory corruption

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

Patch 818.00 continued	• Corrects a problem in AdvFS where a data structure fieldS is not initialized until after an AdvFS mount which is too late. This results in the inability for example to see the files after a remount. • Fixes an AdvFS problem in which the "advfsstat -n" command causes a core dump. The system displays the following error message: Memory fault(coredump) • Fixes a problem that occurs on AdvFS systems. If the "ls -l MI" command is given in a .tags directory, the fileset will become unmountable. If the system is then halted, a panic will occur. • Corrects a problem in AdvFS where a data structure field is not initialized until after an AdvFS mount which is too late. This results in the inability for example to see the files after a remount. • 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 of the following commands: # shutdown now # init s when AdvFS is the root or usr filesystem. • 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: 0xfffffc00006cad90 = "kernel memory fault" • Adds features and corrections to the AdvFS verify utility. • Fixes a problem that occurs on AdvFS systems. The chfsets function returns incorrect exit values and inappropriate error messages.

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

Patch 818.00 continued	• 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 problem that causes a lockmode 4 system panic. • 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 • 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 problem that occurs on AdvFS file systems. A kernel memory fault occurs on the AdvFS file system when accessing nfs-mounted files. • 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 situation where a quotacheck can cause a system panic. • Fixes a problem in which vrestore can cause an occasional core dump (Floating Exception). • 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.

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

Patch 818.00 continued	• Fixes AdvFS performance problems. • Fixes an kernel memory fault panic. The system displays the following error message: trap: invalid memory read access from kernel mode • This patch 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 • Corrects a problem where the mcellCount on-disk was not being updated as files were being migrated and this resulted in a panic situation. • This patch fixes a problem caused by the vrestore command. The command would fail when restoring multiple savesets from a TZS20 tape drive. • Provides a performance improvement for AdvFS systems. • 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 occurred when an AdvFS panic crashed the customer's system but the visible symptom was a crash due to a kernel memory fault. • Adds features and corrections to the AdvFS verify utility. The verify utility now detects and reports some file system corruption problems it had previously ignored. It also no longer gives seek errors on really large frag files (>2GB); gives detailed warning messages when a frag file is found to be incorrectly terminated, helping the user to know which file's fragments are involved; gives a useful error message when the root_domain is mounted read-only, preventing it from investigating other domains; properly handles domains that have clones; and properly handles SBM fixups (code which was intended to correct corrupted pages in the SBM metadata file fixed the page in memory but then wrote the newly corrected page over the NEXT page in the SBM.) Also, increases the amount of memory available to the program so that large memory systems can be worked with.

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

Patch 818.00 continued	• Corrects a panic and hang situation due to a limit of advfs access structures. • 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. • 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 message: 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.

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

Patch 818.00 continued	• 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 • 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 AdvFS that was causing a memory leak. • 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.

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

Patch 818.00 continued	• 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 with AdvFS that caused a page fault and the following panic: panic (cpu 0): kernel memory fault • 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 the AdvFS logging code, The way locking was implemented was causing degraded performance. • 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 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 819.00 OSF405-403A-1	**Patch:** Security (SSRT0546U, SSRT0542U) **State:** Supersedes patches OSF405-400331-1 (339.01), OSF405-102 (274.00), OSF405-400239 (230.00), OSF405-400189 (164.00), OSF405-400250 (229.00), OSF405-999 (373.00), OSF405-440C (797.00), OSF405-403C (799.00) This patch corrects the following: • This update is to replace /usr/shlib/libc.so with /shlib/libc.so in the distributed file list, since the former is really a symbolic link to the latter. Also included in the update is changes to the installation instructions to deal with the hard links, /shlib/libc.so to /shlib/libc_r.so and /usr/ccs/lib/libc.a to /usr/ccs/lib/libc_r.a. • 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. • Fix to libtli/libxti to correctly handle a continuation data message still on the stream head. • 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 820.00 OSF405-403D	**Patch:** Include Corrections, Sec. (SSRT0546U, SSRT0542U) **State:** Supersedes patches OSF405-400331-1 (339.01), OSF405-102 (274.00), OSF405-400239 (230.00), OSF405-400189 (164.00), OSF405-400250 (229.00), OSF405-999 (373.00), OSF405-440C (797.00), OSF405-403C (799.00) This patch corrects the following: • This update is to replace /usr/shlib/libc.so with /shlib/libc.so in the distributed file list, since the former is really a symbolic link to the latter. Also included in the update is changes to the installation instructions to deal with the hard links, /shlib/libc.so to /shlib/libc_r.so and /usr/ccs/lib/libc.a to /usr/ccs/lib/libc_r.a. • 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. • Fix to libtli/libxti to correctly handle a continuation data message still on the stream head. • 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 821.00 OSF405X11-005A	**Patch:** Mach64 Graphics Card Monitor Handling **State:** Supersedes patch OSF405X11-005 (54.00) On systems with an ATI Mach64 graphics card, sometimes the monitor will lose synchronization or become stuck in power-save mode.

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

Patch 822.00 OSF405X11-005B	**Patch:** Mach64 Graphics Card Monitor Handling **State:** Supersedes patch OSF405X11-005 (54.00) On systems with an ATI Mach64 graphics card, sometimes the monitor will lose synchronization or become stuck in power-save mode.
Patch 823.00 OSF405CDE-400013A	**Patch:** Security, (SSRT0498U) **State:** Supersedes patches OSF405CDE-400013 (454.00), OSF405CDE-400013B (591.00) 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 824.00 OSF405CDE-400013C	**Patch:** CDE Environment, Security, (SSRT0498U) **State:** Supersedes patch OSF405CDE-400013-1 (454.01) A potential security vulnerability has been discovered in 'libDtSvc', where under certain circumstances users may gain unauthorized access. DIGITAL has corrected this potential vulnerability.

3

Summary of TruCluster Software Patches

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

Table 3–1 lists patches that have been updated.

Table 3–1: Updated TruCluster Software Patches

Patch IDs	Change Summary
Patches 5.00, 29.00, 34.00, 36.00, 40.00, 41.00, 42.01	Superseded by Patch 51.00
Patches 5.00, 29.00, 34.00, 36.00, 40.00, 41.00, 42.01	Superseded by Patch 52.00
Patches 5.00, 29.00, 34.00, 36.00, 40.00, 41.00, 42.00	Superseded by Patch 46.00
Patches 11.00, 23.00	Superseded by Patch 33.01
Patch 13.00	Superseded by Patch 48.00
Patch 13.00	Superseded by Patch 47.00
Patches 14.00, 22.00, 26.00, 38.00	Superseded by Patch 44.00
Patches 16.00, 39.00, 37.00, 45.00, 43.00	Superseded by Patch 49.00
Patches 16.00, 39.00, 37.00, 45.00, 43.00	Superseded by Patch 50.00

Table 3–2 provides a summary of patches in Patch Kit-0008.

Table 3–2: Summary of TruCluster Patches

Patch IDs	Abstract
Patch 3.00 TCR141-003	**Patch:** Correction For DRD I/O Hangs When No CPU In Slot 0 **State:** Existing This fixes a problem that occurs on all AlphaServer 8200 systems and on AlphaServer 8400 systems having certain nonstandard configurations. When there is no CPU in slot 0, remote DRD I/O operations hang.
Patch 4.00 TCR141-004	**Patch:** Correction For Distributed Lock Manager Hang **State:** Existing This patch fixes a problem that occurrs when MEMORY CHANNEL errors are encountered at the same time that a particular code path is executed. When these events occurr simultaneously, the distributed lock manager (DLM) would hang. The likelihood of this problem occurring is low.

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

Patch 6.00 TCR141-006	**Patch:** tractd Corrections **State:** Existing This patch corrects the following: • Fixes a problem where the Cluster Monitor (cmon) in some cases may display incomplete or incorrect ASE service status and node UP/DOWN status. • Fixes a problem with complete depletion of system socket resources, the result of tractd daemons doing repeated connect retries. This problem is most commonly seen when all nodes in a three- or four-node cluster are booted simultaneously. • Dramatically reduces tractd daemon interconnect delays seen when multiple cluster nodes are booted simultaneously. These delays are reduced from the 5+ minutes range in the case of four node clusters, to just a few seconds. In addition, the interconnects in these circumstances are more reliably complete.
Patch 7.00 TCR141-007	**Patch:** Memory Channel Memory Allocation Corrections **State:** Existing This patch fixes a problem which caused the "map_RM_receive" panic to occur in some cases. This problem may also be seen as distributed raw disk (DRD) print warnings on the console if the drd-mc-drd-print-warn parameter is set in the /etc/sysconfigtab file.
Patch 21.00 TCR141-021	**Patch:** lsm_dg_action Correction **State:** Existing This patch fixes two problems that were causing certain LSM actions to not be retried upon failure, even though the conditions that caused the failures were only temporary.
Patch 24.00 TCR141-009	**Patch:** Network interface and Routing Corrections **State:** Existing This patch fixes the following problems: • During the failover of an ASE service, the removal of the -alias parameter from the /var/ase/sbin/nfs_ifconfig file caused the routing file to become corrupted. • When removing and adding services in an available server environment (ASE) using multiple network interfaces, the gated daemon would be started even when value of the ASEROUTING variable in the /etc/rc.config file is "no."
Patch 25.00 TCR141-025	**Patch:** Distributed Lock Manager Corrections **State:** Existing This patch fixes a problem in TruCluster Production Server Software that can cause a cluster member to panic during a shutdown.
Patch 27.00 TCR141-027	**Patch:** Correction for KZPBA controllers **State:** Existing Without this patch the ase_fix_config utility will not recognize KZPBA controllers.
Patch 28.00 TCR141-028	**Patch:** Correction for KZPBA SCSI controllers **State:** Existing This patch replaces the /usr/sbin/clu_ivp script with a new script that will recognize the "isp" KZPBA SCSI controllers. Without this patch the clu_ivp program will ignore these controllers.

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

Patch 30.00 TCR141DX-002	**Patch:** Cluster Monitor Hang Correction **State:** Existing If an ASE service is renamed, any running Cluster Monitor (cmon) will lockup and hang. This occurs whether the rename was done from within cmon or independent of cmon.
Patch 31.00 TCR141-032	**Patch:** ase_mount_action Correction **State:** Existing Fixes a problem in which running the vquotacheck command on a filesystem participating in an ASE service will cause a system to panic if the service fails over or relocates while the command is in progress.
Patch 32.00 TCR141-033	**Patch:** Booting Node Hang Correction **State:** Existing Fixes a problem where a booting node hangs in the imc_init command. A re-reboot would also hang in imc_init, requiring a reboot of all members.
Patch 33.01 TCR141-034-1	**Patch:** Kern Mem Fault And simple_lock Panic Correction **State:** Supersedes patches TCR141-011 (11.00), TCR141-019 (23.00) This patch corrects the following: • Fixes the following problems in the ASE Availability Manager (AM): – A "simple_lock: time limit exceeded" panic on multi-processor, and system hangs in single processor systems. This can occur when multiple host target mode requests are issued due to SCSI aborts and resets on a shared bus. – A kernel memory fault panic caused by a race condition when the AM de-initializes. • Fixes a kernel memory fault in am_select() in the Availability Manager. • Fixes a problem where the aseagent process goes into a U state when another ASE member leaves the cluster, due to the aseagent process waiting on a SCSI ping request that never completes.
Patch 35.00 TCR141-036	**Patch:** rm_spur Driver Correction **State:** Supersedes patch TCR141-002 (2.00) This patch corrects the following problems: • Eliminates the loss of a cluster node when "sysconfig -q rm" is run after the cluster has formed. • Allows more time to remove a node from an 8-node cluster before causing the system to panic. • Corrects some instances on busy clusters when the software doesn't realize a node has gone down. • Corrects the sense of the long/short heartbeat timeout delay in virtual hub systems, and enables code that allows the system to see a hub power up after it has been powered down.

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

Patch 44.00 TCR141-046	**Patch:** Lock Manager Corrections **State:** Supersedes patches TCR141-014 (14.00), TCR141-022 (22.00), TCR141-026 (26.00), TCR141-040 (38.00) This patch corrects the following: • Fixes a problem in the TruCluster Production Server Software in which a system can panic with: rcv_invvalb_req: value block out of sequence • Two problems in the TruCluster Distributed Lock Manager (DLM): one resulting from a process's effective group ID not being checked when a process attempts to join a namespace, another in which repeated calls to the dlm_quecvt function would erroneously return DLM_LKBUSY status. • An assertion panic that occurs after a large number of transactions are made using the same lock. The assertion panic is triggered by integer wrapping of the lock transaction ID field. The system may panic with "dlm_panic". The actual assertion message is "lk_txid == 0>". • An erroneous assertion involving deadlock search. The system may panic with "dlm_panic". The actual assertion message is "<otxid != (dlm_trans_id_t)-1>". • Fixes a problem that can cause a cluster member to panic in rcv_deqlk_msg() with the panic string set to: dlm_panic • Fixes a system panic with the following message: "snd_grantlk_msg: no memory for message"

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

Patch 46.00 TCR141-044B	**Patch:** Kernel Memory Fault Panic **State:** Supersedes patches TCR141-005 (5.00), TCR141-029 (29.00), TCR141-035 (34.00), TCR141-038 (36.00), TCR141-042 (40.00), TCR141-043 (41.00), TCR141-044 (42.00) This patch corrects the following: • Fixes a problem in the message service routines used by the daemons in TruCluster Available Server and Production Server software. When the message queue fills, the following message is entered in the daemon.log file, but the queue is not emptied: msgSvc: message queue overflow, LOST MESSAGE! From this point on, no further messages will be received. • Fixes the following problems in the ASE Availability Manager (AM): – A "simple_lock: time limit exceeded" panic on multi-processor, and system hangs in single processor systems. This can occur when multiple host target mode requests are issued due to SCSI aborts and resets on a shared bus. – A kernel memory fault panic caused by a race condition when the AM de-initializes. • Fixes a problem where, during an orderly shutdown (init 0), the ASE agent shuts down the director before shutting down the services. • Causes the host status monitor (asehsm) to actively go out and learn current member states before responding to the director with member state information. • Pulling all monitored network interface cables on the machine running the asedirector and a service can result in another machine starting a new director and starting the same service before it has been fully stopped on the first machine. This is especially noticeable when a service takes a long time to stop. • Fixes a problem that caused the asedirector to core dump if asemgr processes were modifying services from more than one node in the cluster at the same time. • Fixes a problem where the Host Status Monitor (asehsm) incorrectly reports a network down (HSM_NI_STATUS DOWN) if the counters for the network interface get zeroed. • Fixes scalability problems in the DECsafe Available Server, TruCluster Available Server and TruCluster Production Server products. The problems caused the asemgr to core dump when adding or modifying services with a large number of disks.
Patch 47.00 TCR141-013B	**Patch:** Memory Channel API Shared Library Correction **State:** Supersedes patch TCR141-013 (13.00) This patch fixes various problems in the MEMORY CHANNEL API. In particular, changes were made to ensure that the API is thread safe, that locks are properly acquired and released, and to increase performance and reliability.
Patch 48.00 TCR141-013-1	**Patch:** Memory Channel API Static Library Correction **State:** Supersedes patch TCR141-013 (13.00) This patch fixes various problems in the MEMORY CHANNEL API. In particular, changes were made to ensure that the API is thread safe, that locks are properly acquired and released, and to increase performance and reliability.

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

Patch 49.00 TCR141-045-1	**Patch:** Support For New AdvFS Mount Option "-o noatimes" **State:** Supersedes patches TCR141-016 (16.00), TCR141-041 (39.00), TCR141-039 (37.00), TCR141-048 (45.00), TCR141-045 (43.00) This patch fixes the following problems: • Provides support in asemgr for the new AdvFS mount option "-o noatimes". • Fixes a problem where changes in the LSM configuration were not being properly handled during the delete of an LSM volume from a service. • Increases the timeout values for the LSM action scripts that are part of the TruCluster Production Server, Available Server and DECsafe Available Server products. The timeouts were too small for large LSM configurations and, under certain conditions, would cause the start of the services to fail, leaving them unassigned. • Fixes a problem in which under certain cercumstances, an ASE service modification could result in a corrupted configuration data base. • Fixes a problem where LSM disk information was not properly updated in the ASE database when volumes were removed from a disk service.
Patch 50.00 TCR141-045B	**Patch:** LSM and AdvFS Corrections **State:** Supersedes patches TCR141-016 (16.00), TCR141-041 (39.00), TCR141-039 (37.00), TCR141-048 (45.00), TCR141-045 (43.00) This patch fixes the following problems: • Provides support in asemgr for the new AdvFS mount option "-o noatimes". • Fixes a problem where changes in the LSM configuration were not being properly handled during the delete of an LSM volume from a service. • Increases the timeout values for the LSM action scripts that are part of the TruCluster Production Server, Available Server and DECsafe Available Server products. The timeouts were too small for large LSM configurations and, under certain conditions, would cause the start of the services to fail, leaving them unassigned. • Fixes a problem in which under certain cercumstances, an ASE service modification could result in a corrupted configuration data base. • Fixes a problem where LSM disk information was not properly updated in the ASE database when volumes were removed from a disk service.

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

Patch 51.00 TCR141-044-2	**Patch:** Not Properly Handling Error Condition Correction **State:** Supersedes patches TCR141-005 (5.00), TCR141-029 (29.00), TCR141-035 (34.00), TCR141-038 (36.00), TCR141-042 (40.00), TCR141-043 (41.00), TCR141-044-1 (42.01) This patch corrects the following: • Fixes a problem in the message service routines used by the daemons in TruCluster Available Server and Production Server software. When the message queue fills, the following message is entered in the daemon.log file, but the queue is not emptied: msgSvc: message queue overflow, LOST MESSAGE! From this point on, no further messages will be received. • Fixes the following problems in the ASE Availability Manager (AM): – A "simple_lock: time limit exceeded" panic on multi-processor, and system hangs in single processor systems. This can occur when multiple host target mode requests are issued due to SCSI aborts and resets on a shared bus. – A kernel memory fault panic caused by a race condition when the AM de-initializes. • Fixes a problem where, during an orderly shutdown (init 0), the ASE agent shuts down the director before shutting down the services. • Causes the host status monitor (asehsm) to actively go out and learn current member states before responding to the director with member state information. • Pulling all monitored network interface cables on the machine running the asedirector and a service can result in another machine starting a new director and starting the same service before it has been fully stopped on the first machine. This is especially noticeable when a service takes a long time to stop. • Fixes a problem that caused the asedirector to core dump if asemgr processes were modifying services from more than one node in the cluster at the same time. • Fixes a problem where the Host Status Monitor (asehsm) incorrectly reports a network down (HSM_NI_STATUS DOWN) if the counters for the network interface get zeroed. • Fixes scalability problems in the DECsafe Available Server, TruCluster Available Server and TruCluster Production Server products. The problems caused the asemgr to core dump when adding or modifying services with a large number of disks.

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

Patch 52.00 TCR141-044C	**Patch:** Message Service Routine Fixes **State:** Supersedes patches TCR141-005 (5.00), TCR141-029 (29.00), TCR141-035 (34.00), TCR141-038 (36.00), TCR141-042 (40.00), TCR141-043 (41.00), TCR141-044-1 (42.01) This patch corrects the following: • Fixes a problem in the message service routines used by the daemons in TruCluster Available Server and Production Server software. When the message queue fills, the following message is entered in the daemon.log file, but the queue is not emptied: msgSvc: message queue overflow, LOST MESSAGE! From this point on, no further messages will be received. • Fixes the following problems in the ASE Availability Manager (AM): – A "simple_lock: time limit exceeded" panic on multi-processor, and system hangs in single processor systems. This can occur when multiple host target mode requests are issued due to SCSI aborts and resets on a shared bus. – A kernel memory fault panic caused by a race condition when the AM de-initializes. • Fixes a problem where, during an orderly shutdown (init 0), the ASE agent shuts down the director before shutting down the services. • Causes the host status monitor (asehsm) to actively go out and learn current member states before responding to the director with member state information. • Pulling all monitored network interface cables on the machine running the asedirector and a service can result in another machine starting a new director and starting the same service before it has been fully stopped on the first machine. This is especially noticeable when a service takes a long time to stop. • Fixes a problem that caused the asedirector to core dump if asemgr processes were modifying services from more than one node in the cluster at the same time. • Fixes a problem where the Host Status Monitor (asehsm) incorrectly reports a network down (HSM_NI_STATUS DOWN) if the counters for the network interface get zeroed. • Fixes scalability problems in the DECsafe Available Server, TruCluster Available Server and TruCluster Production Server products. The problems caused the asemgr to core dump when adding or modifying services with a large number of disks.