DIGITAL UNIX

Patch Kit-0004 for Version 3.2DE2
Release Notes and Installation Instructions

March 1998

Product Version: DIGITAL UNIX Version 3.2DE2

This manual describes the contents of Patch Kit-0004, describes how to install and remove patches, and provides other information that you need to know when working with patch kits for the DIGITAL UNIX operating system software.

Digital Equipment Corporation
Maynard, Massachusetts

Contents

About This Manual

This manual contains information specific to Patch Kit-0004 for the DIGITAL UNIX Version 3.2DE2 operating system software. It describes how to install and remove this kit, and provides other information you need to know when working with DIGITAL UNIX patch kits.

Audience

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

Organization

This manual is organized as follows:

Chapter 1 Provides an overview of the concepts and features of the patch kits.

Chapter 2 Introduces the `dupatch` utility and provides information to be aware of when installing patches.

Chapter 3 Contains the release notes for this patch kit.

Chapter 4 Describes the installation procedures for the patch kit.

Chapter 5 Contains general DIGITAL UNIX system upgrade information.

Chapter 6 Summarizes the patches included in the kit.

Chapter 7 Provides samples for installing patches, viewing patch documentation, and setting a system baseline.

Related Documentation

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

- *Installation Guide*
- *System Administration*
- Any release-specific installation documentation.

Reader's Comments

DIGITAL 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:

Digital Equipment 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 DIGITAL technical support office. Information provided with the software media explains how to send problem reports to DIGITAL.

1

Introduction

This chapter provides an overview of the concepts and features of the DIGITAL UNIX patch kits.

1.1 Overview

The DIGITAL UNIX patch kits contain official patches for critical problems in the DIGITAL UNIX operating system software. These kits, which are distributed as needed, provide interim maintenance that prevents the occurrence of known critical problems in the DIGITAL UNIX Version operating system. The patch kits contain the following elements:

- Version-specific patches and patch-specific documentation, including release notes and installation instructions
- A patch-management utility for installing, viewing, deinstalling, and managing patches

Note

Patch kits are not intended to provide general maintenance and new functionality; applying them to your system does not obviate the need to upgrade to later versions of DIGITAL UNIX.

1.1.1 Applicability of Patch Kits

Patch kits are applicable to a specific version of DIGITAL UNIX, unless stated otherwise in the patch kit release notes. This patch kit will not install on any other version of DIGITAL UNIX.

1.1.2 Patch Kit Contents

Each DIGITAL UNIX operating system patch kit contains the following components:

- Installation instructions and release notes

  This manual also contains an overview of new features and other pertinent information.

- Patch management utility (`dupatch`)

  Installs, deinstalls, and manages `setld`-installed official patches for the DIGITAL UNIX operating system. This utility is installed and left on the system through the successful installation of a DIGITAL UNIX operating system patch kit. It is automatically updated if a later patch kit contains a new version of the utility.

- Patch subsets
- Patch-specific documentation

  Contains information that is installed and left on the system in `/var/adm/patch/doc` through the use of a DIGITAL UNIX operating system patch kit. The following documentation is included for each patch:

  - Patch abstract, which summarizes the patches
  - Patch README file, which contains a description of the problems that the patch corrects
- Patch kit installation tools

1.2 Patch Kit Packaging

A patch is a collection of files. Patches are merged together, into one patch, if they have intersecting files or co-dependencies. A patch may correct one or more problems.

Each patch is packaged in its own `setld` subset. The subsets are managed by a utility named `dupatch`.

Each patch kit contains all of the DIGITAL UNIX version-specific patches available at the time of its manufacturing. You can selectively install and deinstall each patch.

DIGITAL UNIX patches are provided in two different packages:

- Aggegrate selective installation patch kit

  Aggregate kits contain all of the DIGITAL UNIX version-specific patches available for distribution at the time of its manufacturing. You can selectively install and deinstall each patch through the use of `dupatch`, which is included in each kit.
- Singular patch kit

  The primary content of a singular patch kit is one patch. To ensure proper installation and system consistency, any dependent patches are included in the kit. Therefore, a singular patch kit may include one or several patches, depending upon the inter-patch dependencies.

  Installation is accomplished through the use of `dupatch`, which is included in every patch kit.

The patch kit is delivered as a tar file that you unpack on the target system or on a file system on a network that is accessible by the target system. Once the patch kit is unpacked, you run `dupatch` to install, deinstall, and manage official patches for the DIGITAL UNIX operating system. After you install the patches, the following items are left on the system:

- The `dupatch` utility.
- Patch-specific documentation that you can view with `dupatch`
- Optionally, the archived system files that were updated by the installed patches

1.3 Patch Kit Naming

Patch kit names have the following syntax:

product | version| kit_type | kit# | -mfg_date | .file_ type

The following list describes the attributes currently used in patch kit names:

product DU = DIGITAL UNIX

version V40

V40A

V40B

V40C

V40D

V32C

V32DE1

V32DE2

V32F

V32G

kit_type AS=Aggregate Selective installation patch kit

SS =A patch kit containing a single patch

kit# The numeric identifier that DIGITAL uses to track the kit contents. For example, this booklet is for Patch Kit-0004.

mfg_date The year, month, and day the kit was changed

.file_type .tar

The following example shows the name of an aggregate patch kit for DIGITAL UNIX Version 4.0B, patch kit-0002, manufactured on May 1, 1997:

```
DUV40BAS00002-19970501.tar
```

The following example shows the name of a single-patch kit for DIGITAL UNIX Version 4.0B, patch 97.00, patch kit-0002, manufactured on May 1, 1997:

```
DUV40BSS0000200009700-19970501.tar
```

1.4 Patch Kit Installation Requirements

To successfully install this patch kit, your system must meet the following requirements:

- Be running the appropriate version of DIGITAL UNIX
- Contain the necessary temporary and permanent storage space described in Section 3.1.

2

Features and Restrictions

This chapter introduces you to the dupatch utility for installing, deinstalling, and managing patches. It also provides information you must be aware of when installing patches.

2.1 Patch Management Utility

All official patches are installed, deinstalled, and managed through the setld-based patch management utility dupatch. Because dupatch manages patch interdependencies, direct setld installations and deinstallations (setld -l -d) are disabled.

Directions for enabling or disabling patches are provided after the successful installation or deinstallation of all selected patches (for example, kernel rebuild and system reboot).

Every time dupatch is run a session log that captures dupatch activities is created. It is located in /var/adm/patch/log/session.log. Up to 25 copies of the session log is saved. The order is first in, first out.

A patch event log, located in /var/adm/patch/log/event.log, captures the patching events for this system.

When you run the system baseline feature, the baselining log is captured in /var/adm/patch/log/baseline.log. Up to 25 copies of the baselining log are saved; the order is first in, first out.

With dupatch, you can perform the following actions:

- Install and deinstall all or selected patches
- View the patch-specific documentation on your system and on the available patch kit
- Display the current dupatch installed patches on the system
- Display all patched files on the system

2.2 Command Line User Interface

This version of dupatch contains a command line interface that allows dupatch to be called by other programs. You can use the command line to invoke all functions except for baselining. The functions have the same operation and definition as the menu-driven interface. For an operation to be completely noninteractive, you must specify all mandatory switches on the command line or in the data_file file.

The following list shows all of the command line interface options (typing dupatch -help provides the same information):

```
dupatch -delete
        -name<user_name>
        -note<user_note>
        -name<all | patch_id{patch_id...]>

    [Optional switches]
```

```
        -data<data_file>
        -root<root_patch>
        -proceed  ( Proceed with patches that passed predeletion check)
        -version<version_string>

dupatch -help

     [Optional switches]
        -data  (Specifies data_file use)
        -patch_id  ( Specifies patch_id use)
        -rev  (Lists dupatch version)
        -version_string  (Specifies version_string use)

dupatch -install
        -kit<kit_location>
        -name<user_name>
        -note<user_note>
        -patch<all | patch_id[patch_id...]>  (Optional when -prechec_only is specified)

    [Optional switches]

        -data<data_file>
        -nobackup
        -precheck_only
        -proceed  (Proceed with patches that passed preinstallation check)
        -rood<root_path>
```

Using a Data_file

When using the -data switch, you must specify a data_file, which is a file path that contains specifications with the following format:

```
switch1=value
switch2=value
    .
    .
    .
switch3
```

For example:

```
kit = /mnt
name = John Doe
note = install April patch kit
patch = all

precheck_only
nobackup
```

The following list describe characteristics of a data_file:

- Blank lines and comments (preceded with #) are allowed.
- Line continuation (\) is required if a specification spans multiple lines.
- When a switch is specified both on the command line and in the data_file, the value specified on the command line overrides that specified in the data-file.

Using a patch_id

The following list describes the characteristics of a patch_id:

- A valid patch_id specification has the following format:

  'all' xxxx[.yy]

  For example:

```
200.11
10.2
00111.02
```

- xxxx is the patch identifier and yy is the patch revision
- Both xxxx and yy are numeric values; leading zeros can be omitted.
- Patch revision (yy), when left unspecified, maps to wildcarded "??"
- Multiple patch_id specifications are separated by white space.
- The keyword `all` cannot be combined with other patch_ids.

Using a root_path

The following list describes the characteristics of a root_path:

- The `-root` switch, which is similar to the `-D` switch of `setld`, specifies an alternative root for the specified operation.
- The root_path must be the root of a complete DIGITAL UNIX file system.
- The default root_path is / for all operations.

Using Version Strings

The following list provides valid DIGITAL UNIX version strings:

```
V3.2C
V3.2D-1/E-1
V3.2D-2/E-2
V3.2F
V3.2G
 V4.0
V4.0A
V4.0B
V4.0C
V4.0D
```

The following list describes characteristics of version strings:

- A version_string specification only applies to the patch_id specifications that follow it and ends when another version_string is specified.
- A version_string specification is not necessary when the patch_id specification contains no ambiguities.
- Because the purpose of the version_string is to clarify the patch_id specification, its specification must precede that of the patch_id.

Example:

```
-version V4.0 -patch 1.1 -version V4.0B -patch 1.1
```

In a delete operation, if only one patch 1.1 is installed on your system, the `-version` switch is not required.

2.3 Inventory Management of Patched File Changes

Using a `setld`-based installation utility to install patches enables the tracking of official DIGITAL UNIX operating system patch activity such as the following:

- Tracking current `setld`-installed patches on the system
- Ensuring correct handling of customized system configuration files so that customizations are not lost (for example, `conf.c`). These files are also referred to as system-protected files (`.new.`)
- Validating patch applicability to existing system files (collision detection)

Patch applicability to the existing system files is done on a file-by-file basis for each patch. This ensures that the installation of a patch will not degrade or crash the system. The installation of a patch is blocked if any system files to be replaced by a patch are not valid predecessors of the patch files.

Patch applicability also enables consistency checking and reporting for operating system patch installation.

In all cases where a patch is blocked, informative messages are provided to assist you in determining how to proceed.

The installation of a patch is blocked if the following conditions exist:

- The underlying operating system product subset is not installed
- The `setld` inventory is inconsistent with the existing system files. This occurs when an operating system product `setld` subset is installed and individual operating system files that are part of that subset are moved or deleted.
- Any of the existing system files (files on the system that are targeted for update by the patch) have changed and cannot be related to previous versions of this patch. This ensures that operating system files that change due to other explicit system administrator action (for example, layered product or test patch installations) are not inadvertently overwritten. You must take special action to enable patch installation in this situation. For more information see Section 2.6.

2.4 Patch Reversibility

Utilizing `dupatch` for patch installation allows you to revert the system to its state prior to the installation of a particular patch. To revert a patch, you must enable the Reversibility installation option for that patch.

By default, the Reversibility installation option is set to enable Reversibility for patches. If you choose to make patch subsets nonreversible, then those patches will become nonremovable upon the successful installation of those patches.

Patch reversibility is dependent upon saving the existing system files that will be updated by the patch. Saving these files requires the availability of adequate storage space in `/var/adm/patch/backup`, which can be a mount point for a separate disk partition, an NFS mount point, or a symbolic link to another file system. This provides maximum user configurability to reduce the impact on system disk space for the `/`, `/usr`, and `/var` partitions.

To further reduce the storage space required to save existing system files, the patch kits for DIGITAL UNIX save the files in a compressed tar image per each patch. DIGITAL UNIX 4.n releases use the `gzip` utility to save the files in a compressed tar image per each patch; this results in a file with a name like *`filename.tar.gz`*. DIGITAL UNIX Version 3.2x releases use the `compress` utility to save the files in a compressed tar image per each patch; this results in a file with a name like *`filename.tar.Z`*. The file name is the patch subset name that replaced the system files.

The `dupatch` utility checks for the required storage space prior to patch installation.

2.5 Optional Multiuser Patch Installation Preparation

You must be in single-user mode for the installation phase of DIGITAL UNIX operating system patches. However, the following activities can be done in multiuser mode:

- Untar the patch kit
- View patch documentation
- Select and verify patch installation

  Note that while in multiuser mode, you cannot verify the space needed for the kernel to rebuild or that your kernel will rebuild.
- View which `setld`-installed patches exist on your system

2.6 Establishing a Patch Baseline for Your System

You will need to set the baseline for your system if you have manually installed test patches, early release patches, or official patches. Manually installed patches or any changed operating system files may block official `setld`-based patches from installing.

The `dupatch` utility contains a feature that enables your system to be baselined for routine use of `setld`-based patch kits. This feature is broken into several phases that assess and report the state of your operating system files. It will only make changes to your system with your confirmation. Section 7.3 contains a sample baselining session.

Warning

Enabling the `dupatch` baselining feature to update your system sets a new baseline for your operating system software environment. You will not be able to revert to previous operating system software states. It is recommended that you backup your `/`, `/usr`, and `/var` file systems prior to enabling system updates through this feature.

The baselining phases are as follows:

- Phase 1 - System Evaluation

  Where possible, this phase determines the origin of changed operating system files and detects previously released official patches that were manually installed.
- Phase 2 - Report patches with layered product conflicts

  Some layered products ship operating system files. If any such files exist on your system, they will show up during this phase. You cannot install patches that intersect with a layered product because the patch would corrupt the layered product operation.
- Phase 3 - Create installation records for manually installed patches

  During this phase, you will be shown a list of patches that match the operating system files on your system. You will be offered an opportunity to mark these patches as installed on your system. This involves copying valid `setld` database information to your system.
- Phase 4 - Report changed system files not included in the patch kit

  This phase provides information to help you make choices later in this process. The files that appear in this phase are changed on your system but their origin cannot be determined. They are also not part of the patch kit under evaluation. You will want to consider this information when you later make decisions in phase 5.
- Phase 5 - Enable patches with file conflicts or missing system files

This phase allows you to enable subsequent installation of patches whose inventory does not match the installed system. This occurs under the following conditions:

– When system files change and the origin of that change cannot be determined

– When the original file to be patched is missing from the system

It is recommended that you do not enable the installation of these patches until you have tracked down the origin of the files that are in conflict.

To assist you in this effort, the file list for the entire patch with the known information will be displayed. You can run through this phase to get the analysis without enabling the installation of any of the listed patches.

Warning

It is important to ascertain why the operating system files have changed prior to enabling patches to overwrite them. Failure to do so may cause your operating system software environment to be in an inconsistent state.

2.7 Restrictions

The following sections describe information you must be aware of when installing or deinstalling patches.

2.7.1 DIGITAL UNIX Operating System Patches Must Be Applied in Single-User Mode

The installation phase of DIGITAL UNIX patch kits require the system to be in single-user mode to ensure computing environment integrity. Patch selection and pre-installation checking can be accomplished in multiuser mode. However, the actual installation must be done in single-user mode. Minimally a system reboot is required to complete the installation and bring the system to a consistent running environment. Certain file types, such as libraries, are not moved into place until you reboot the system.

2.7.2 Impact on System Upgrades to Later Versions of DIGITAL UNIX

In the presence of patches or layered products, certain procedures used to upgrade a system to a later version of DIGITAL UNIX can lead to an inconsistency among operating system and layered product objects. For more information see Chapter 5 for general DIGITAL UNIX system upgrade information.

Note

After successfully installing a new version of DIGITAL UNIX, you should obtain and install the latest patch kit that is applicable to that version of DIGITAL UNIX.

2.7.3 Root Access Is Required to Install and Deinstall Patch Kits

Installation and deinstallation of patches requires root or superuser access to the system.

2.7.4 No RIS or DMS Installation of Patches

Remote Installation Services (RIS) and Dataless Mangement Services (DMS) installations of patches are not supported. However, the patch kit installation mechanism does support network installation via NFS.

2.7.5 Direct setld Installation and Deinstallation of Patch Subsets Is Not Allowed

You can install and deinstall patches only through `dupatch`. You cannot directly install or reinstall the patch subsets with `setld`. This ensures that patch tracking and management is not compromised.

2.7.6 Limitation for /var/adm/patch/backup Directory Handling

The patch management utility assumes there is one `/var/adm/patch/backup` directory per system. It does not handle placement of archived original files for multiple systems in one directory.

2.7.7 No Ctrl/c During Installation Phase

Do not enter a Ctrl/c command during the installation phase of the patch kit.

Warning

As with any system update, entering a Ctrl/c during this phase will leave the operating system software environment in an inconsistent and nonrecoverable state.

2.7.8 Deleting Patches Containing Customized Files

If you use `dupatch` to delete a patch containing a customized file, messages similar to the following may appear in the session log file, `/usr/var/adm/patch/log/session.log`:

```
Customization found in <pathname_of_patched_file_deleting>.
Before the backup was restored, we had saved a copy of this file in:

   <pathname_of_patched_file_deleting>.PreDel_OSFPAT<patch_subset_ID_no.>

Please compare <pathname_of_file_replacing_patched_file> with this saved copy.
If there are extra customizations you want to keep, you would need

to merge them into <pathname_of_file_replacing_patched_file> manually.

   <pathname_of_patched_file_deleting>.PreDel_OSFPAT<patch_subset_ID_no.>

can be removed afterwards."
```

This message warns you to examine the deleted patch for any customized files it may contain. In order to keep those customizations, you will have to manually add them.

The following are examples of such customized files:

- `/usr/var/spool/cron/crontabs/root`
- `/etc/sysconfigtab`
- `/usr/var/adm/sendmail/sendmail.cf`

3

Release Notes

This chapter provides information that you must be aware of when working with Patch Kit-0004.

3.1 Required Storage Space

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

- 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 ~34.9 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 Section 2.4 for more information.

  Up to ~35.5 MB of storage space in /var/adm/patch may be required for original files if you choose to install and revert all patches. See Section 2.4 for more information.

  Up to ~580 KB of storage space is required in /var/adm/patch/doc for patch abstract and README documentation.

  A total of ~72 KB of storage space is needed for the patch management utility.

3.2 Upgrading a Patched DIGITAL UNIX Version 3.2DE2 System

If you are upgrading your patched Version 3.2DE2 system to a later version of DIGITAL UNIX, you must be aware of the following information:

- If you are upgrading to Version 4.0 or higher through a new installation or an update installation, you do not have to deinstall any patches. This type of upgrade replaces all operating system files, including your customized files.
- If you are upgrading to Version 3.2F or Version 3.2G via direct setld loading (sparse inventory kit), you will need to remove some previously installed patches. This type of upgrade only replaces some operating system files and preserves your customized operating system files (see Chapter 5 for more information.

  You must remove the following patches:

  – 8.00 (OSF365–008)
  – 60.00 (OSF365–360024)
  – 362.00 (OSF365–360125)
  – 167.00 (OSF365–350213)
  – 171.01 (OSF365–350221–1)
  – 208.00 (OSF365–350284)
  – 218.00 (OSF365–350298)

- 251.00 (OSF365X–350015)
- 274.00 (OSF365–350336)
- 302.00 (OSF365–350374)
- 311.00 (OSF365–360082B)
- 312.00 (OSF365–360082C)
- 317.00 (OSF365–350384)
- 325.00 (OSF365–063)
- 346.00 (OSF365–075)
- 351.00 (OSF365–350431)
- 353.00 (OSF365–350440)
- 357.00 (OSF365–350449)

This patch kit forces these patches to be reversible, regardless of your answer to the question “Do you want the patches to be reversible? [y]”. This is done to ensure that you can properly upgrade your system to a later version of DIGITAL UNIX.

The affected patches may change as new patches are made to DIGITAL UNIX Version 3.2DE2. This list will be updated and managed for each patch kit.

4

Installation Instructions

This chapter provides installation instructions for DIGITAL UNIX operating system patch kits.

4.1 Preparing to Install Patches

Before you install Patch Kit-0004 make sure that your system meets the required criteria and that you perform certain preinstallation tasks, as described in the following sections.

4.1.1 Required System Software

You must have DIGITAL UNIX Version 3.2DE2 installed on your system to install this patch kit. It will not install on any other version of DIGITAL UNIX.

4.1.2 Backing Up Your System

It is recommended that you backup your /, /usr, and /var file systems prior to installing this patch kit.

4.1.3 Setting System Baseline for Setld-Based Patch Kits

You will need to set the baseline for your system if you have manually installed test patches, early release patches, or official patches. Manually installed patches or any changed operating system files may block official setld-based patches from installing. See Section 2.6 and Section 7.3 for more information.

4.2 Installing and Enabling Patches

Installing patches requires the following steps:

1. Placing the updated system files in the appropriate areas on the system disk
2. Enabling the use of those patched files

DIGITAL UNIX operating system patch kits provide a setld-based patch management utility that places the updated system files in the appropriate areas with the proper owner, group, permissions, and required links to other system files.

Patch-enabling instructions are provided after all selected patches are installed. In general the patch-enabling instructions are as follows

- If kernel patches are installed, you must do a kernel rebuild and a system reboot. Explicit user action is required to rebuild and use the new kernel. Refer to your DIGITAL UNIX *Installation Guide* for instructions on rebuilding and using the new kernel
- If commands, utilities, or library patches are installed, you must reboot the system. A system reboot is required to complete the installation and bring the system to a consistent running environment. For example, certain file types, such as libraries, are not moved into place until the system is rebooted.

- If a user-customizable file is patched, you must manually merge the new and existing versions of those files prior to rebuilding the kernel.
- If a patch delivers new features the accompanying online patch-specific documentation or the release notes provide further system or patch configuration information.

  Any special patch instructions are noted at the beginning of the preinstallation and installation sessions.

4.2.1 Installation and Enabling Instructions

Patch installation is performed through `dupatch`. The `-l` and `-d` options to the `setld` command are disabled for patch subsets. Sample local installation steps to install DIGITAL UNIX operating system patches:

1. Ensure the installation prerequisites described in Section 4.1 are met.
2. In multiuser mode, log into the system as root or become superuser.
3. Make the patch kit available to the system by either mounting the remote file system in which it is located or by copying it to the system.

   Enter the following command to mount the file system that contains the patch kit on `/mnt`:

   /usr/sbin/mount*yourfilesystem* **/mnt**

   To untar the patch kit onto the system, you need to create a file system that has the required space. See Section 3.1 for storage space requirements. It is recommended that this file system not exist in `/usr or /var`. For example:

   ```
   # mkdir /tmp/pkit
   # cd /tmp/pkit
   # tar -xpvf /mnt/DUV40BAS00003-19970425.tar
   ```

4. You can proceed in one of two ways from this point:
   - You can stay in multiuser mode to select patches for installation and perform only a preinstallation check. Then at an appropriate time shut the system down to single-user mode and perform the installation of the patches. If you choose this method, proceed to step 5.
   - You can shut down the system to single-user mode to perform the patch selection, preinstallation check, and installation. If you choose this method proceed to step 9.
5. To continue in multiuser mode and perform patch selection and preinstallation checks, run `dupatch` from the newly untarred kit. For example:

   ```
   # /tmp/pkit/dupatch
   ```

   This results in the installation of the required patch tools subset and presentation of the following menu:

   ```
   DIGITAL UNIX Patch Utility
   ==========================
   (This dupatch session is logged in /var/adm/patch/log/session.log)

   Main Menu:
   ----------
   1) Patch Installation
   2) Patch Deletion

   3) Patch Documention
   4) Patch Tracking

   5) Patch Baseline Analysis/Adjustment
   ```

```
h) Help on Command Line Interface

q) Quit
Enter your choice: 1
```

6. Enter 1 for Patch Installation. The following menu is presented:

```
DIGITAL UNIX Patch Utility
==========================
(This dupatch session is logged in /var/adm/patch/log/session.log)

 Patch Installation Menu:
 ------------------------

1) Pre-Installation Check ONLY
2) Check & Install (requires single-user mode)

b) Back to Main Menu
q) Quit

Enter your choice: 1
```

7. Enter 1 to have the program run a preinstallation check. See Chapter 7 for installation examples. You will be asked to submit the following information:

```
Your name
Enter path to the patch kit (the directory containing ./kit and ./doc subdirectories):
Do you want the patches to be reversible? [y]:
Do you want to proceed with the installation with this setup? [y/n]:
```

8. Select and verify the patches to install through the patch selection menus. Once patch selection is done, `dupatch` performs the preinstallation checking and reports the results. Refer to the installation examples in Chapter 7.

   You can proceed to the installation phase when it is convenient to shut the system down to single-user mode. Proceed to step 9.

9. Shut down the system to single-user mode. For Example:

   # **/usr/sbin/shutdown +5 "Applying Patch Kit-0001"**

   To reboot to single-user mode from the console prompt, issue a command like the following:

   >>>**boot -fl s**

10. After the system shuts down to single-user mode, mount the file system that contains the `/usr` and `/var` directories. Use the `bcheckrc` command to check and mount all the UFS and AdvFS file systems, then issue the `update` command and activate your swap partition with `swapon`:

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

    If you are using the Logical Storage Manager, you should also run `lsmbstartup`:

    # **/sbin/lsmbstartup**

11. If you need access to the network, use the following command to start the network:

    # **/usr/sbin/rcinet**

    Informational messages will appear on the screen.

12. Run the patch management utility to install the patches:

    # **dupatch**

```
DIGITAL UNIX Patch Utility
==========================
(This dupatch session is logged in /var/adm/patch/log/session.log)
```

```
Main Menu:
----------

1) Patch Installation
2) Patch Deletion

3) Patch Documention
4) Patch Tracking

5) Patch Baseline Analysis/Adjustment

h) Help on Command Line Interface

q) Quit

Enter your choice: 1
```

13. Enter 1 to install the patch kit. The following menu is presented:

```
DIGITAL UNIX Patch Utility
==========================
(This dupatch session is logged in /var/adm/patch/log/session.log)

Patch Installation Menu:
------------------------

1) Pre-Installation Check ONLY
2) Check & Install (requires single-user mode)
b) Back to Main Menu
q) Quit
Enter your choice: 2
```

14. Enter 2 to have the program check your system and install the patch kit. See Chapter 7 for installation examples. You will be asked to respond to the following:

```
Your name
Enter path to the patch kit (the directory containing ./kit and ./doc subdirectories):
Do you want the patches to be reversible? [y]:
Do you want to proceed with the installation with this setup? [y/n]:
```

15. Select and verify the patches to install through the patch selection menus. Once you have finished the patch selection, `dupatch` performs the preinstallation checking and installation. See Chapter 7 for installation examples.

    Informational messages will appear on the screen. The dupatch session is logged as the informational messages may scroll off of the screen. To ensure that the installation was successful, review the `dupatch` session log for special patch instructions, informational, and error messages. The log file is located in `/var/adm/patch/log/session.log`.

16. If there are no error messages, you should follow the instructions for enabling the patches that are in the session log. Depending upon the installed patches you may need to merge customized files, rebuild the kernel, or simply reboot the system to enable the installed patches.

4.2.2 Deinstalling and Disabling Patches

Deinstalling patches requires two steps:

- Removing the patched system files and replacing them with the prior versions of those files
- Disabling the use of the patched files

Patch Kit-0004 provides a `setld`-based patch management utility that is capable of deinstalling patches if the revert option was selected when the patch was installed.

Patch-disabling instructions are provided after all selected patches are removed. In general, the patch-disabling instructions are as follows:

- If kernel patches are deinstalled, you must do a kernel rebuild and a system reboot. Explicit user action is required to rebuild and use the new kernel. Refer to your DIGITAL UNIX *Installation Guide* for instructions on rebuilding and using the new kernel.
- If commands, utilities, or library patches are deinstalled, you must reboot the system. A system reboot is required to complete the deinstallation and bring the system to a consistent running environment. For example, certain file types, such as libraries, are not moved into place until the system is rebooted.
- The prior version of user-customizable files are restored and do not require any explicit action.

4.2.3 dupatch Delete Menu

The `dupatch` Delete menu applies to all `setld`-based patches installed on your system; it does not focus on any specific patch kit. This menu allows you to delete a specific patch, a list of patches, or all patches from your system.

The Delete menu lists every `setld`-based patch on your system, regardless of which patch kit installed them. Therefore, if you select the **delete all patches** menu item, it will remove all `setld`-patches from your system.

For example, if chose the **install all patches** menu item when installing Patch Kit-0004 and then decided to remove those patches, you would have to specifiy the patch ID of all Patch Kit-0004 patches in the Delete menu. If, instead, you select the **delete all** menu item, then all `setld`-based patches that were installed on your system would be deleted, not just those from Patch Kit-0004.

4.2.4 Patch Deinstallation and Disabling Instructions

Patch deinstallation is performed through `dupatch`. The `-l` and `-d` options to the `setld` command are disabled for patch subsets. The system must be in single-user mode to deinstall patches. The following example shows the steps used to deinstall patches:

1. Shut down the system to single-user mode. For Example:

   # **/usr/sbin/shutdown +5 "Deinstalling Patches"**

2. After the system shuts down to single-user mode, mount the file system that contains the `/usr` and `/var` directories. Use the `bcheckrc` command to check and mount all the UFS and AdvFS file systems. Then issue the `update` command and activate your swap partition with `swapon`:

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

   If you are using the Logical Storage Manager, you should also run `lsmbstartup`:

   # **/sbin/lsmbstartup**

3. If you need access to the network, use the following command to start the network:

   # **/usr/sbin/rcinet start**

   Informational messages will appear on the screen.

4. Run `dupatch`, select `2` for patch removal:

```
# dupatch


DIGITAL UNIX Patch Utility
==========================
(This dupatch session is logged in /var/adm/patch/log/session.log)

Main Menu:
----------

1) Patch Installation
2) Patch Deletion

3) Patch Documention
4) Patch Tracking

5) Patch Baseline Analysis/Adjustment

h) Help on Command Line Interface

q) Quit

Enter your choice: 2
```

5. Select and verify the patches to deinstall through the patch selection menus. Once patch selection is done, `dupatch` performs deinstallation of patches. Informational messages will appear on the screen. The `dupatch` session is logged as the informational messages may scroll off of the screen.
6. To ensure the deinstallation was successful review the `dupatch` session log for special patch instructions, informational, and error messages. The log file is located in `/var/adm/patch/log/session.log`.
7. If there are no error messages, you should follow the instructions for enabling the patches that are in the session log. Depending upon the installed patches you may need to merge customized files, rebuild the kernel, or simply reboot the system.

4.2.5 Verifying the Installation or Deinstallation of Patches

Verify patch installation or deinstallation by reviewing the `dupatch` session log for informational and error messages.

5

DIGITAL UNIX System Upgrade Information

This chapter provides background information on DIGITAL UNIX system upgrades in the presence of operating system patches. Releases of DIGITAL UNIX are structured and distributed as full or sparse inventory kits.

5.1 Full Inventory DIGITAL UNIX Kit

This type of kit contains a full inventory of operating system objects (headers, libraries, kernel modules, and the like). It can be used to perform full and update installations:

- A full (also called new) installation creates new file systems and loads a full copy of DIGITAL UNIX from the kit onto a system. Any other version of DIGITAL UNIX, any layered products, and any patches that previously existed on the system are overwritten. A full installation does not preserve system customizations (for example, user or data files) because the root (/), `/usr`, and `/var` file systems are re-created during the process.
- An update installation from a full inventory kit loads a full copy of DIGITAL UNIX from the kit, replacing every operating system object that existed on the system prior to the installation.

  An update installation does not update layered products. This may cause a regression in operation of a layered product if a layered product version of a DIGITAL UNIX object is replaced with a new version of that object.

The end result of either a full or an update installation is an operating system consisting of a known set of operating system objects that provides predictable system behavior.

Following an update installation it is necessary to install all layered products and all DIGITAL UNIX patches (official as well as test) that were built for the new release.

5.2 Sparse Inventory DIGITAL UNIX Installation

The DIGITAL UNIX Version 3.2C family sparse inventory operating system kits do not contain a full inventory of operating system objects. Also, it does not use either the full or the update installation processes described above; it uses setld directly.

Because a sparse inventory kit contains only a partial inventory of DIGITAL UNIX objects, installing from this type of kit does not load an entire copy of DIGITAL UNIX onto a system. Existing objects are overwritten only if replacement objects exist on the software kit.

Sparse inventory kits are produced assuming that any system to be upgraded is running the baseline DIGITAL UNIX operating system objects from a previous release. In the presence of patches, a layered product that modifies base operating system files and other files causes the system to deviate from one of the supported baselines and has the potential to cause object inconsistency following an installation from a sparse inventory kit. Therefore, you must exercise special care when upgrading DIGITAL UNIX from a sparse inventory kit.

Following a sparse inventory installation, you must install all appropriate versions of layered products and all DIGITAL UNIX patches (official as well as test) that were built for the new release. Failure to do so will probably cause a regression in the behavior of layered products, DIGITAL UNIX, or both.

The following tables provide upgrade information for the V3.2, V3.2C, and V4.0 families of releases.

Table 5–1: Upgrade Migration for DIGITAL UNIX Version 3.2 Family

DIGITAL UNIX Version	Kit Type	Upgrade Migration Supported
V3.2	Full	From V3.0, V3.0A, V3.0B via an update installation.
V3.2A	—	This release consisted of layered products only.
V3.2B	Sparse	This release provided V3.2 functionality for new hardware.
V3.2C	Full	From V3.2, V3.2A, V3.2B via an update installation.
V3.2D-1	Sparse	From V3.2C via `setld`.
V3.2E-1	Sparse	From V3.2D-1 via `setld`. This release contains DIGITAL UNIX fixes necessary for TruCluster V1.0 to function.
V3.2D-2	Full	No migration path. Full installation only for AlphaServer 2100A.
V3.2E-2	Sparse	From V3.2D-2 via `setld` This release contains DIGITAL UNIX fixes necessary for TruCluster V1.0 to function.
V3.2F	Sparse Full	From V3.2C, V3.2D-1 via `setld`. No migration path. Full installation only for AlphaServer 4100.
V3.2G	Sparse	From V3.2C, V3.2D-1, V3.2D-2, V3.2E-1, V3.2E-2, V3.2F via `setld`.

Table 5–2: Upgrade Migration for DIGITAL UNIX Version 4.0 Family

DIGITAL UNIX Version	Kit Type	Upgrade Migration Supported
V4.0	Full	From V3.2C, V3.2D-1, V3.2D-2 via update installation
V4.0A	Full	From V3.2G or V4.0
V4.0B	Full	From V4.0A
V4.0C	Full	Installs only on DIGITAL Personal Workstation 433AU and DIGITAL Personal Workstation 500AU

6

Summary of Patches

This chapter summarizes all of the patches included in Patch Kit-0004.

Table 6–1 lists patches that have been updated.

Table 6–1: Updated Patches

Patch IDs	Change Summary
Patch 295.00	Superseded by Patches 315.00, 361.00, 362.00
Patch 38.00	Superseded by Patch 335.00
Patch 299.00	Superseded by Patch 325.00
Patch 313.00	Superseded by Patch 237.00
Patches 36.00, 43.00, 226.00, 291.00, 292.00, 339.00	Superseded by Patches 328.00, 337.00, 352.00, 339.01, 344.00, 356.00, 342.00, 343.00, 346.00
Patch 300.00	Superseded by Patch 302.00
Patch 238.00	Superseded by Patch 326.00
Patch 44.01	Superseded by Patches 334.00, 353.00
Patch 286.00	Superseded by Patch 329.00
Patch 250.00	Superseded by Patch 331.00
Patch 340.00	Superseded by Patch 357.00. 282.00
Patch 94.01	Superseded by Patch 327.00
Patch 290.00	Superseded by Patch 347.00
Patch 181.00	Superseded by Patch 348.00
Patch 230.00	Superseded by Patch 349.00
Patche 198.01	Superseded by Patch 351.00
Patch 275.00	Superseded by Patch 354.00
Patch 212.00	Superseded by Patch 355.00
Patch 298.00	Superseded by Patch 360.00

Table 6–2 provides a summary of patches in Patch Kit-0004.

Table 6–2: Summary of patches in Patch Kit-0004

Patch IDs	Abstract
Patch 8.00 OSF365-008	**Patch:** Multi-PCI Bus Systems Don't Config Loadable Drivers **State:** Existing This patch fixes a problem where a system with more than one PCI bus will fail to configure the loadable device drivers.
Patch 11.00 OSF365-011	**Patch:** RAID Set Dump Device, No Crash Dump After Panic **State:** Existing Fixes a problem where a system, with a RAID set for a dump device, will not save the crash dump to the RAID set after a panic.
Patch 25.00 OSF365-025	**Patch:** Crash-dumps To Non-re0 RAID Devices **State:** Existing Crash-dumps to non-re0 RAID devices broken on all PCI & EISA machines.
Patch 30.00 OSF365-030	**Patch:** ioctl() Using The TIOCM_RI Mask Always Fails **State:** Existing An ioctl() system call within a user application will fail if the TIOCM_RI flag is passed as an argument to this system call.
Patch 39.00 OSF365-039	**Patch:** psiop Driver Corrections **State:** Supersedes patches OSF365-006 (6.00), OSF365-024 (24.00) This patch corrects the following: • A problem that occurs with the NCR 53C8XX driver (psiop) in which the device may not appear to be on the SCSI bus. • Data corruption due to change in DNAD register behavior on Symbios 810A/825A/860/875 chips. • At boot, when probing the psiop driver, the system may continuously loop generating the following error message: "siopintr: interrupt for non-initialized controller"
Patch 42.00 OSF365-042	**Patch:** Token Ring Driver Corrections **State:** Supersedes patch OSF365-023 (23.00) This patch corrects the following: • This patch fixes a Token Ring transmission timeout. The driver can experience "ID 380PCI20001 (8/13/95)" as described in the TI380PCI Errata. • The token ring driver, when storing the product_id, can cause corruption which can result in a kernel read access panic.
Patch 60.00 OSF365-360024	**Patch:** Corrections For NFS Loopback Mounts & UBC **State:** Supersedes patch OSF365-350104 (108.00) This patch corrects the following: • Fixes a problem where processes will hang in an uninterruptable state while using NFS loopback mounts. • Kernel memory fault in ubc_sync_iodone().

Table 6–2: Summary of patches in Patch Kit-0004 (cont.)

Patch 75.00 OSF365-360050	**Patch:** nfs Mounted Filesystems Correction **State:** Supersedes patches OSF365-360003 (48.00), OSF365-360037 (68.00) • A problem in which PATHWORKS client does not see all the files in a directory when the directory is an NFS mounted OpenVMS UCX exported directory. • Fixes a problem in which mmap activity to a file that is NFS mounted may cause the client process to hang after the file is deleted. • Large memory growth of ucred structures can occur. This is especially prevalent if a user is using setuid programs.
Patch 84.00 OSF365-360062	**Patch:** ar Command Option Correction **State:** Existing The ar command's -x option, which extracts archive files, may, in error, return a message stating that the file was not found.
Patch 85.00 OSF365-360064	**Patch:** Quota Support For Numeric User Names And Groups **State:** Existing This patch 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. It also provides new options to allow them to specify userids and groupids.
Patch 95.01 OSF365-350061-1	**Patch:** Security Correction, rdist (SSRT0329U) **State:** Existing A potential security vulnerability has been discovered, where under certain circumstances users may gain unauthorized access. DIGITAL has corrected this potential vulnerability.
Patch 97.00 OSF365-350073	**Patch:** bootp Server Daemon Correction **State:** Existing The bootp daemon appends a null character to file names in its responses.
Patch 98.00 OSF365-350079	**Patch:** allocate more timeout Correction **State:** Existing Fixes "timeout table overflow" panic on multiprocessor system.
Patch 101.00 OSF365-350089	**Patch:** tftpd Server Command Correction **State:** Existing Corrections to tftpd when using interface aliases, bind() uses the client's address received rather than INADDR_ANY. This fix accomodates bootpd when used with ASE for failover purposes.
Patch 104.00 OSF365-350096	**Patch:** acctcms Hash Table Overflow Correction **State:** Existing Fixes acctcms hash table overflow error.
Patch 105.00 OSF365-350097	**Patch:** prog trans w FreePort Express Correction **State:** Existing Program translated with FreePort Express (SunOS –> DIGITAL UNIX) binary translator does not run correctly.
Patch 107.00 OSF365-350102	**Patch:** libexc Process Signal Mask Corruption Correction **State:** Existing Program using libexc.a suffer corrupted signal masks.

Table 6–2: Summary of patches in Patch Kit-0004 (cont.)

Patch 110.00 OSF365-350109	**Patch:** NFS Server Duplicate Request Correction **State:** Existing Correct nfs server duplicate request problem, by adding timestamps.
Patch 111.00 OSF365-350111	**Patch:** tip Command Correction **State:** Existing Running tip(1) consumes about 45% of cpu time, resulting in no idle time, even if tip is about the only thing running on the system.
Patch 112.00 OSF365-350112	**Patch:** Security, lattelnet Correction **State:** Existing A potential security vulnerability has been discovered where under certain circumstances users may gain unauthorized access. DIGITAL has corrected this potential vulnerability.
Patch 114.00 OSF365-350115	**Patch:** ATM IP Correction **State:** Existing Card lockup problem using the ATM IP convergence module.
Patch 119.00 OSF365-350136	**Patch:** Kernel Memory Fault: u_anon_free() Routine **State:** Existing The system panics with kernel memory fault, and the fault_pc is in the u_anon_free() routine.
Patch 120.00 OSF365-350139	**Patch:** UFS Memory Mapping Corrections **State:** Supersedes patch OSF365-350054 (93.00) This patch corrects the following: • "ufs_getapage: allocation failed" panic. • Applications that continuously map and unmap large data files hang in uninterruptable state.
Patch 122.00 OSF365-350143	**Patch:** call-share Segmentation Fault Correction **State:** Existing A call-share executable with a text, data or bss region greater than 4 gbytes, the application will segment fault.
Patch 123.00 OSF365-350144	**Patch:** Peer Server & Token Ring Source Routing Correction **State:** Existing Using Peer Server 1.3 ECO1 and token ring network interface(s), source routing discovery is not working as expected. Additional interfaces will not initialize and links between remote stations cannot be established.
Patch 128.00 OSF365-350152	**Patch:** Security, (SSRT0376X) **State:** Existing A potential security vulnerability has been discovered, where under certain circumstances users may "gain unauthorized access" to the system. DIGITAL has corrected this potential vulnerability.
Patch 136.00 OSF365-350169	**Patch:** Common Agent mold Consumes Avail Virtual Memory **State:** Existing The mold daemon component of the Common Agent leaks memory when running with the DEC SNA PeerServer product.
Patch 141.00 OSF365-350176	**Patch:** find Command ffm Set Correction **State:** Existing This patch fixes a problem where the find command returns a invalid status code upon encountering a file in an "ffm" set.

Table 6–2: Summary of patches in Patch Kit-0004 (cont.)

Patch 147.01 OSF365-350185-1	**Patch:** Incorrect NIS passwd dbm File Permission **State:** Existing After yppasswd has been run, NIS passwd dbm files will have read and write permissions for other users.
Patch 148.00 OSF365-350186	**Patch:** strsetup Command Correction **State:** Existing This patch resolves a problem with "strsetup -i -f" creating duplicate major and minor numbers.
Patch 151.00 OSF365-350190	**Patch:** sysfs: Function Not implemented (add ffm & nfsv3) **State:** Existing This patch adds support for file system ids ffm and nfsv3.
Patch 152.00 OSF365-350191	**Patch:** Remote Execution Server (rexecd) Correction **State:** Existing This patch resolves the condition that results when there is no default shell in the password file causing rexecd to fail.
Patch 157.00 OSF365-350198	**Patch:** rcp Command Correction (handling >2GB File) **State:** Existing This patch fixes a problem in which the rcp program fails when the file being copied is greater than 2 Gigabytes in size. The error message from rcp is: "connection closed".
Patch 159.01 OSF365-350200-1	**Patch:** df Command Correction **State:** Existing This patch fixes a problem in which the output from the df command displays incorrectly formatted columns.
Patch 164.00 OSF365-350206	**Patch:** ping -ff Segmentation Fault **State:** Existing This patch corrects the problem where "ping -p ff" results in a segmentation fault and core dump.
Patch 165.00 OSF365-350210	**Patch:** ypserv, ypbind Corrections **State:** Existing NIS slaveservers will not accept a push from the master server of a new map.
Patch 166.00 OSF365-350211	**Patch:** Kernel Mem Fault Panic (route.o) **State:** Supersedes patch OSF365-350197 (156.00) This patch corrects the following: • Resolves a problem which causes kernel memory fault in ubc_sync_iodone(). • Fixes a problem in which the system panics when the routing code failed to range check the destination address length.

Table 6–2: Summary of patches in Patch Kit-0004 (cont.)

Patch 167.00 OSF365-350213	**Patch:** LSM Corrections **State:** Supersedes patches OSF365-350065 (96.00), OSF365-350243 (188.00), OSF365-350244 (189.00) This patch corrects the following: • A problem in which an LSM configuration database becomes corrupted when it grows beyond 128 KB. The LSM daemon displays an error message similar to the following when it starts up: bad magic number • A problem with vold not detaching a disk when the kernel fails a plex. • A problem where vold core dumps in ASE. Happens when there is a SCSI reservation conflict. • Fixes several problems that occur during certain LSM operations involving disklabel changes.
Patch 168.00 OSF365-350216	**Patch:** volrecover -b Command Correction **State:** Existing This patch fixes a problem that occurs when the -b option of the volrecover command is used. The problem is that a background job spawned to perform the recovery operation fails when a SIGHUP signal is received.
Patch 170.00 OSF365-350218	**Patch:** Memory Leak Due to automount Command **State:** Existing Automount program has a memory leak. In some cases, this leak can cause applications to hang. The daemon.log file shows the following error message: "Memory allocation failed: not enough space"
Patch 171.01 OSF365-350221-1	**Patch:** MFA Driver ESP Self-test Halt/Restart **State:** Existing This patch fixes a halt/restart problem with the mfa driver ESP self-test.
Patch 173.00 OSF365-350223	**Patch:** Security, rpc.pcnfsd (SSRT0396U) **State:** Supersedes patch OSF365-350175 (140.00) This patch corrects the following: • A potential security vulnerability has been discovered in the rpc.pcnfsd program, where under certain circumstances users may gain unauthorized access. DIGITAL has corrected this potential vulnerability. All customers should install this patch. • This patch fixes problems with the rpc.pcnfsd program that can cause rpc.pcnfsd to crash. This patch also fixes a problem where pcnfsd does not generate audit events for successful pcnfsd authorizations.
Patch 174.01 OSF365-350224-1	**Patch:** Support for New European Timezones **State:** Existing Fix European timezones for new EC (European Community) rules for daylight savings time.
Patch 177.00 OSF365-350230	**Patch:** Wrong Default uid/gid From cd_defs Library **State:** Existing This patch corrects a problem with the cd_defs() function of libcdrom where cd_defs(CD_GETDEFS) returns the wrong default gid and uid for an ISSO 9660 CD-ROM.

Table 6–2: Summary of patches in Patch Kit-0004 (cont.)

Patch 178.00 OSF365-350231	**Patch:** inode Calc Err Of /dev/fd Correction **State:** Existing System V getdirentries() system call did not correctly calculate the number of entries in a directory inode when accessing the /dev/fd file system.
Patch 183.00 OSF365-350237	**Patch:** find Command Corrections **State:** Existing The find command will not handle more than 100 arguments.
Patch 184.00 OSF365-350238	**Patch:** uux Command Correction **State:** Existing The uux command generates error messages when input is generated from stdin jobs. This occurs in many cases where uucp was used to send mail.
Patch 185.00 OSF365-350239	**Patch:** ksh Shell Corrections **State:** Supersedes patches OSF365-350162 (133.00), OSF365-350171 (137.00) This patch corrects the following: • When editor options are set in ksh, ksh would formerly would not reset modes when ksh exited via a trap. • A problem in which a system running ksh as the login shell would wipe out the previous contents of the history file (for example, .sh_history) and put the new information in the file. This occurred after a user logged into an ULTRIX system from a DIGITAL UNIX system using the telnet or rlogin commands. • This patch fixes a problem where an attribute had been set to "read-only", and it could not be set back (unset) to "read/write" status by using the built-in command typeset of the ksh (e.g., typeset +r).
Patch 186.00 OSF365-350240	**Patch:** showmount Command Corrections **State:** Existing This patch corrects the following: • Add the time out options -t nnn & -T to the 'showmount' command. • "showmount -e host" command does not receive the requested export list from the specified host within 25 seconds, and issues the following error message: Can't do Exports rpc: RPC: Timed out
Patch 187.00 OSF365-350241	**Patch:** pfm Driver Corrections **State:** Existing This patch corrects the following: • The pfm driver does not provide any profiling data on CPUs other than #0. • The uprofile and kprofile commands, on EV4/EV5 systems, may cause the system to hang or to provide incorrect data.
Patch 191.00 OSF365-350247	**Patch:** acctcom Command Correction **State:** Existing Fixes a problem in which the size field of a process displayed by the acctcom command is displayed incorrectly.

Table 6–2: Summary of patches in Patch Kit-0004 (cont.)

Patch 193.01 OSF365-350249-1	**Patch:** Kernel LMF Corrections **State:** Supersedes patch OSF365-350249 (193.00) This patch corrects the following: • Permits kernel components to release license units that have been allocated through lmf_auth_ex().
Patch 194.00 OSF365-350251	**Patch:** Invalid Kernel Address Correction **State:** Existing System panics with a kernel memory fault in k_mem_fault by a user application that passes an invalid kernel address as one of the arguments.
Patch 195.00 OSF365-350252	**Patch:** STREAMS Corrections **State:** Supersedes patches OSF365-350204 (162.00), OSF365-350229 (176.00) This patch corrects the following: • This patch allows a customer-written device driver to return the customer's own local error value. Without this patch, the user process will get EINVAL instead. This patch also corrects the situation in which a system could hang after Patch OSF365-350229 is installed. • Fix panic (kernel memory fault) associated with the STREAMS code when stopping layered products. • This patch changes the function that pushes a module on the stream so that the device pointer value is set to the value of the device number saved in the stream head instead of incorrectly setting it to zero.
Patch 199.00 OSF365-350256	**Patch:** sh And rsh Command Corrections **State:** Existing This patch fixes two 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.
Patch 200.00 OSF365-350263	**Patch:** Mail "From" Incorrect On Incoming Remote Mail Msgs **State:** Existing Mail from non-local senders appears to be from "daemon" rather than the person who originated the mail.
Patch 202.00 OSF365-350268	**Patch:** mkpasswd Command Correction **State:** Existing This patch 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.
Patch 203.00 OSF365-350269	**Patch:** Process Hang On SMP System **State:** Existing 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.

Table 6–2: Summary of patches in Patch Kit-0004 (cont.)

Patch 204.00 OSF365-350271	**Patch:** Duplicate namecache Entries Correction **State:** Existing This patch prevents duplicate namecache entries on SMP systems. Under heavy filesystem lookup operations this can eventually result in a simple lock timeout and a system panic.
Patch 205.00 OSF365-350273	**Patch:** rmt Command Of LT 1024 Bytes Correction **State:** Existing The rmt program does not accept reads/writes of less than 1024 bytes and system displays error message: 'Cannot set socket receive buffer size'
Patch 206.01 OSF365-350275-1	**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 207.00 OSF365-350278	**Patch:** /rdump Command Corrections **State:** Existing When a member of the group "operator" logged into the console and dump was invoked with the -n option, an extraneous file (/dev/:0) was created.
Patch 208.00 OSF365-350284	**Patch:** Client-based pseudo-ttys Correction **State:** Supersedes patch OSF365-360043 (71.00) This patch corrects the following: • 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. • This patch addresses kernel memory fault panics seen in systems running with clist-based pseudo-ttys. The kernel memory faults occur either during unrelated malloc() calls, or in calls to proc_ref() from ttymodem().
Patch 209.00 OSF365-350285	**Patch:** more Command Correction **State:** Existing When typing 'more a_particular_file' there is garbage displayed on the screen, while displaying files having lines ending with ^M character.
Patch 210.00 OSF365-350286	**Patch:** Funneled Non-Timeshared Thread Correction **State:** Existing This patch fixes a system hang problem that may occur when a non-timeshared thread running on a multi-processor system is inappropriately given a priority boost when returning from a funneled subsystem.
Patch 211.00 OSF365-350287	**Patch:** Floating Pnt Errs On Programs Compiled w/IEEE mode **State:** Existing This patch 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.

Table 6–2: Summary of patches in Patch Kit-0004 (cont.)

Patch 213.00 OSF365-350289	**Patch:** Compiler Correction **State:** Existing This patch fixes the problem of producing incorrect codegen sequences when doing stack allocation within procedure prologs in which the size of the stack was very large. This problem produced a "Segmentation fault (core dumped)" error message.
Patch 214.00 OSF365-350291	**Patch:** at Command Correction **State:** Supersedes patch OSF365-350233 (180.00) This patch corrects the following: • A problem that occurs on multi-processor 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 problem in which cron jobs will not run if there is an unfinished job in another queue. This problem occurs even if the queue for the job is empty.
Patch 215.00 OSF365-350293	**Patch:** wall & ntalkd Hang When LAT Terminal Device Closes **State:** Existing Processes such as wall or ntalkd, when connected to LAT terminal devices, are hanging when attempting to close, possibly because the LAT sessions have been disconnected abnormally.
Patch 217.00 OSF365-350297	**Patch:** Corrections For Symbolic Link to / **State:** Existing 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.
Patch 218.00 OSF365-350298	**Patch:** OSF365-350298 **State:** Supersedes patches OSF365-350093 (103.00), OSF365-350267 (201.00) This patch corrects the following: • On systems running enhanced security, the login process may fail with a segmentation fault. • A security vulnerability has been discovered when running enhanced security that may facilitate unauthorized users gaining access to the system. DIGITAL has corrected this vulnerability. • On a system running enhanced security, a person may still login on a terminal that has been locked or on which a login failed due to excessive attempts.
Patch 220.00 OSF365-350301	**Patch:** ping Command Can Time Out After rcinet restart **State:** Existing This patch fixes a problem in which the ping command can time out after invoking the "rcinet restart" command.

Table 6–2: Summary of patches in Patch Kit-0004 (cont.)

Patch 222.00 OSF365-350304	**Patch:** Security (SSRT0383U) & PC NFS, rpc.statd Corrcts **State:** Supersedes patch OSF365-350178 (143.00) This patch corrects the following: • Fixes a problem that occurs in ASE/TCR environments in which the rpc.statd daemon does not start when using the -p option to specify a long pathname (> 45 characters). When this happens, NFS locking to the NFS service fails causing applications like mail to hang. • A potential security vulnerability has been discovered in 'rpc.statd', where under certain circumstances users may gain unauthorized access. DIGITAL has corrected this potential vulnerability.
Patch 224.00 OSF365-350306	**Patch:** Corrections For Various Keyboards **State:** Supersedes patch OSF365-350245 (190.00) This patch corrects the following: • On systems with PCXAL, LK411, and similar keyboards, sometimes the keyboard stops working. • On systems with PCXAL, LK411, and similar keyboards, after logging out of a session on the workstation monitor, sometimes the keyboard stops working. A reboot is required to clear the problem.
Patch 225.00 OSF365-350308	**Patch:** ATM Corrections **State:** Supersedes patches OSF365-350187 (149.00), OSF365-350226 (175.00) This patch corrects the following: • Prevents a panic that can occur after deleting an ATM ARP entry. The user command to delete an ATM ARP entry is "atmarp -d". Subsequent access to the ATM ARP table can cause the panic. • Resolves the panics that occur when more than one entry is in an ATM ARP cache bucket. • Resolves a kernel mem fault in atm_arp_manager when duplicate entries exist in the ARP table.
Patch 227.00 OSF365-350114	**Patch:** Assembler Correction **State:** Existing This patch fixes a problem with assembler which was causing the following error message while trying to assemble a valid program: as1: Internal: filename, line ###: st_pdn_idn: idn (huge_integer) less than 0 or greater than max (111)
Patch 228.00 OSF365-350313	**Patch:** Kernel Memory Fault Panic Correction **State:** Existing This patch fixes a problem that occurs when the system panics with the following error message: kernel memory fault
Patch 231.00 OSF365-350317	**Patch:** Network Socket Problem **State:** Existing This patch fixes a network socket problem with select() missing state changes on clients from non-write to writable.

Table 6–2: Summary of patches in Patch Kit-0004 (cont.)

Patch 232.00 OSF365-350318	**Patch:** ftp Command Correction **State:** Supersedes patch OSF365-350090 (102.00) This patch corrects the following: • This patch 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. It is recommended that this patch be installed on all OSF systems. • ftp with .netrc file does not use ACCOUNT FIELD information.
Patch 234.00 OSF365-350322	**Patch:** telnet Corrections **State:** Supersedes patch OSF365-350140 (121.00) This patch corrects the following: • A problem where telnet dumps core if the USER environment variable is the last variable in the environment list. • Telnet may change terminal characteristics and cause application problems if you have set up terminal mode emulation for 8 bits/no-parity. Telnet will override this setting and give you 7 bits/no-parity as the default. This patch also fixes the speed table (QAR 41709) and speed definitions (QAR 25953).
Patch 236.00 OSF365-350331	**Patch:** Security, sendmail (SSRT0421U) **State:** Supersedes patch OSF365-350254 (197.00) This patch corrects the following: • Error in Sending mail get both mail and error messages where the error messages do not correctly describe problem. • sendmail command loops endlessly trying to get a "tf" control file in /var/spool/mqueue. • A potential security vulnerability has been discovered with the sendmail command, where under certain circumstances, users may gain unauthorized access. DIGITAL has corrected this potential vulnerability. • Mail cannot be sent to usernames consisting of uppercase and lowercase letters. • Mail fails when a large distribution list is used.

Table 6–2: Summary of patches in Patch Kit-0004 (cont.)

Patch 237.00 OSF365-360114	**Patch:** Host MIB And SNMP Correction **State:** Supersedes patches OSF365-360026 (61.00), OSF365-360054 (79.00), OSF365-360066 (86.00), OSF365-360100 (313.00) This patch corrects the following: • Removes support for atTable, so that common applications (like NetView autodiscovery) will use the ipNetToMediaTable instead. 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. • Fixes memory leaks with the FDDI and Token Ring method routines used with Extensible SNMP subagent (ESNMP). • The Host MIB code uses incorrect presentation names for some processors. This is seen when retrieving the MIB variable "hrDeviceDescr". This patch also adds presentation names for processors. • This patch allows the extensible SNMP deamon to handle a very high volume of SNMP trap requests. • This patch is a general upgrade for eSNMP components.
Patch 239.00 OSF365-350334	**Patch:** DE425 On EISA, Device Configuration Problems **State:** Existing A system that boots and runs OK with 3 DE425s on an eisa bus may hang during boot if a 4th DE425 is added to the bus. 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.
Patch 241.00 OSF365X-003	**Patch:** Corrections For S3 Trio64 Graphics Cards **State:** Supersedes patch OSF365X-002 (240.00) This patch corrects the following: • Systems with an S3 Trio64 graphics card can loose time (on the order of a few minutes a day). • Fixes a situation where a system with an S3 Trio64 graphics card set at 1280x1024 resolution does not correctly display the cursor.
Patch 243.00 OSF365X-350006	**Patch:** X Font Server Crash Correction **State:** Existing Fixes swapping of ListFontsWithXInfo reply.
Patch 248.00 OSF365X-350011	**Patch:** X Server Display PostScript Correction **State:** Existing Fixes problem with X server DPS gray ramp.
Patch 251.00 OSF365X-350015	**Patch:** xdm, XAddPixel, Security, (SSRT0368U) **State:** Supersedes patches OSF365X-350005 (242.00), OSF365X-350008 (245.00) This patch corrects the following: • A potential security vulnerability has been discovered, where under certain circumstances users may gain unauthorized access. DIGITAL has corrected this potential vulnerability. • XAddPixel problem with ZPixmap and TrueColor. • xdm can't manage more than 8 displays on DIGITAL UNIX V3.2F.

Table 6–2: Summary of patches in Patch Kit-0004 (cont.)

Patch 254.00 OSF365-350130	**Patch:** STRLOG Concatenation Of Sequential Outputs **State:** Existing When using the command /usr/sbin/strace to get STREAMS event trace messages from STREAMS drivers and modules via the STREAMS log driver (strlog), this patch fixes a STRLOG bug which causes concatenation of sequential outputs.
Patch 255.00 OSF365X-350019	**Patch:** User Not Added To New Group Correction **State:** Existing If a new group is added with XSysAdmin and then tries to use XIsso to add the user into the new group, the group shows up but the user never gets added.
Patch 256.00 OSF365X-350020	**Patch:** Slow X Server Performance Drawing Arcs **State:** Existing X server performance is slow when an application is drawing arcs which are outside the bounds of the drawable window.
Patch 257.00 OSF365X-350021	**Patch:** Security, libXt **State:** Existing A potential security vulnerability has been discovered in 'libXt', where under certain circumstances users may gain unauthorized access. DIGITAL has corrected this potential vulnerability.
Patch 258.00 OSF365-350138	**Patch:** Correction For VM Tuning Parameter Change Panic **State:** Existing When a user changes virtual memory (vm) tuning parameters due to slow performance and reboots the machine, the system panics.
Patch 259.00 OSF365X-350023	**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 (or when using a print filter) that can not handle escape sequences.
Patch 260.00 OSF365-360116	**Patch:** "vquotacheck -a" Erroneously Sets Quotas **State:** New patch Fixes a problem where the AdvFS filesystem command "vquotacheck -a" erroneously sets all quotas for users to values derived from the last AdvFS fileset in /etc/fstab, rather than the correct values for each individual fileset.
Patch 261.00 OSF365X-350025	**Patch:** Bookreader Hang Correction **State:** Existing Bookreader hangs 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).
Patch 265.00 OSF365-350149	**Patch:** Long copy of >10MB Files (PW-OSF Srv/WfW Clnt) **State:** Existing Big files (>10MB) take longer to copy to and from a PW-OSF server to a WfW client than to a WNT server (NETbeui transport only).
Patch 266.00 OSF365-350155	**Patch:** LAT Limits Number Of Nodes To 100 **State:** Existing Fixes a problem where the LAT subsystem limits the number of remote LAT nodes on a DIGITAL UNIX system to a maximum of 100.

Table 6–2: Summary of patches in Patch Kit-0004 (cont.)

Patch 268.00 OSF365X-350032	**Patch:** Problems Using ATI Mach64 Graphics Cards **State:** Supersedes patches OSF365X-350010 (247.00), OSF365X-350016 (252.00) This patch corrects the following: • On systems with an ATI Mach64 graphics card, sometimes the monitor will lose synchronization or become stuck in power-save mode. • On an AlphaStation 400 with two ATI Mach64 CX graphics cards (dual-screen), the display on the second screen is corrupted at 1280x1024 resolution. • Fix dashed lines on ATI Mach64.
Patch 269.00 OSF365-360078	**Patch:** cam_tape Correction **State:** Supersedes patch OSF365-360052 (77.00) This patch corrects the following: • Fixes a "simple_lock: time limit exceeded" panic originating from either: – ctape_close() routine – ctape_strategy() routine • Fixes "simple_lock: time limit exceeded" panics coming from ctape_close() or ctape_strategy() routines.
Patch 270.00 OSF365-360081	**Patch:** getty Command Option Correction **State:** Existing Allows getty to accept uppercase usernames.
Patch 272.00 OSF365-049	**Patch:** DE500-XA Halts Under Heavy System/Network Load **State:** Supersedes patch OSF365-022 (22.00) This patch corrects the following: • Fixes system panics on an SMP system with a tu (Tulip) Ethernet interface with error message, "System Uncorrectable Machine Check 660 (retry set)". • Fix bug where packet reception on the DE500-XA PCI Fast Ethernet interface (device mnemonic "tu") comes to a halt under heavy system and network load.
Patch 273.00 OSF365-350335	**Patch:** Security, ftp (SSRT0448U) **State:** Supersedes patches OSF365-350160 (249.00), OSF365-350300 (219.00) 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. • ftpd core dumps when using anonymous ftp with the ls commmand. • A security issue in which a user using anonymous ftp could be logged in to the root directory.

Table 6–2: Summary of patches in Patch Kit-0004 (cont.)

Patch 274.00 OSF365-350336	**Patch:** Threads Corrections **State:** Supersedes patch OSF365-350105 (46.00) This patch corrects the following: • Corrects a problem where multi-threaded applications will experience a hang on SMP systems. • Threaded applications have a tendency to exhaust memory before non-threaded applications do. This patch corrects the thread -afe memory allocator.
Patch 278.00 OSF365-350345	**Patch:** Corrects A UFS file System Performance Problem **State:** Existing Data written to a file greater than 32 GB in length will be slower than data written to the file when it is less than 32 GB in length.
Patch 280.00 OSF365-350351	**Patch:** Security, talkd (SSRT0446U) **State:** Existing A potential security vulnerability has been discovered in talkd, where under certain circumstances, system integrity may be compromised. DIGITAL has corrected this potential vulnerability.
Patch 281.00 OSF365-350352	**Patch:** Corrects Several rpc.lockd Problems **State:** Existing This patch corrects the following: • 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 and the system displays the following error message: NFS error 48 cannot bind sockets
Patch 283.00 OSF365-350357	**Patch:** fsck op, prop list corruption Correction **State:** Supersedes patch OSF365-350347 (279.00) This patch corrects the following: • Fixes fsck operation where if 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. • Fixes a problem in which the UFS property list can become corrupted.
Patch 284.00 OSF365-350359	**Patch:** dd Command Corrections **State:** Existing Fixes a problem in which the dd command can corrupt output on very large files (2 GB or greater) when the "conv=sparse" option is used.
Patch 285.00 OSF365-350362	**Patch:** mailx Command Corrections **State:** Existing Fixes an error that occurs when replying to a message in which the "CC:" field contains blank-separated names not enclosed in angle brackets ("<...>").

Table 6–2: Summary of patches in Patch Kit-0004 (cont.)

Patch 294.00 OSF365-360089	**Patch:** Panics With Panic String "Simple Lock:" **State:** Existing Fixes a problem that could cause the system to panic displaying the following panic string: "Simple_lock: hierarchy_violation."
Patch 296.00 OSF365X-350033	**Patch:** dxsession Close Button Operation Correction **State:** Existing Fixes problem where exiting from the DECwindows Session Manager (dxsession) via the 'Close' option of the window menu results in an undesirable saving of dxsession's scratch file in /tmp. Use of this button also causes a behavior inconsistent, with dxsession's 'End Session' button.
Patch 297.00 OSF365-350161	**Patch:** Kernel Mem Fault In dl_set_timer Panic **State:** Existing Corrects a "kernel memory fault" system panic in the routine dl_set_timer().
Patch 302.00 OSF365-350374	**Patch:** Library Corrections **State:** Supersedes patches OSF365-350199 (158.00), OSF365-350315 (229.00), OSF365-350368 (300.00) This patch corrects the following: • Fixes a problem for TLI applications which make use of the t_accept library routine. The secondary endpoint state is not being set correctly. • Corrects a problem encountered by tli applications which do an abort disconnect on an endpoint which was established as an orderly release endpoint and leave the endpoint in an unexpected state. • The problem of t_rcv NOT setting the error flag (t_errno) when no data is retrieved. • Applies to the tli and xti library routines t_rcvrel and t_sndrel. The t_rcvrel routine does not work properly in the T_DATAXFER state; it returns T_OUTSTATE. The t_sndrel routine incorrectly returns a T_LOOK error.
Patch 306.00 OSF365-360095	**Patch:** telnetd Correction **State:** Existing Prevents a long delay while trying to log out using telnet.
Patch 307.00 OSF365-350378	**Patch:** Corrects ibcurses tparm Routine **State:** Existing Fixes a problem in which the tparm routine in the libcurses.a library does not support more than a three digit value for its input parameter.
Patch 308.00 OSF365-360097	**Patch:** Misc nfs_client problems **State:** Existing Fixes a problem in which the system crashes when attempting to NFS mount a text file.
Patch 309.00 OSF365-360098	**Patch:** Pipe Function Correction **State:** Existing Fixes the pipe function, occurs primarily on SMP systems, that exits prematurely causing data errors.
Patch 311.00 OSF365-360082B	**Patch:** OSF365-360082B **State:** Existing Fixes a potential security vulnerability in BIND.

Table 6–2: Summary of patches in Patch Kit-0004 (cont.)

Patch 312.00 OSF365-360082C	**Patch:** Utility Corrections **State:** Existing Fixes a potential security vulnerability in BIND.
Patch 316.00 OSF365-350383	**Patch:** syslogd Cannot Write /dev/console **State:** Supersedes patch OSF365-350188 (150.00) This patch corrects the following: • Fixes a problem where 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. • After a login session on /dev/console exits, syslogd cannot write to /dev/console.
Patch 317.00 OSF365-350384	**Patch:** Various Sckt, Net, pcktfltr, panic Corr **State:** Supersedes patches OSF365-350084 (263.00), OSF365-350146 (125.00), OSF365-350151 (127.00), OSF365-350151-1 (127.01), OSF365-350158 (131.00), OSF365-350192 (153.00), OSF365-350193 (154.00), OSF365-350195 (155.00), OSF365-350248 (192.00), OSF365-350294 (216.00), OSF365-350305 (223.00), OSF365-350319 (233.00), OSF365-350338 (276.00), OSF365-350342 (277.00), OSF365-055 (305.00), OSF365-057 (310.00) This patch corrects the following: • Enhanced fix to the solockpair() routine; problem symptoms include kernel memory faults with sockets, mbufs and mblocks as well as hangs. Applications using sockets in a multi-threaded, multi-cpu environment can experience a number of lock violations with the socket structures. • Fixes a problem in which packet filter programs do not receive packets when the source is sending multicast packets on an Ethernet network. • 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 • Fixes situation of a DIGITAL UNIX system connected to a token ring network receiving a ping, not being able to respond and the token ring driver displays "List Error in transmit" message. • 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. • A kernel fix for network sockets left in FIN_WAIT_1 state forever. This patch contains a "tunable" kernel parameter. It is recommended that only experienced system administrators attempt to set this parameter from the default value. • A "panic: lock_read: hierarchy violation in del_dealloc_stg" error occurs when a socket lock is held by a UNIX domain while calling vrele().

Table 6–2: Summary of patches in Patch Kit-0004 (cont.)

Patch 317.00 continued	• Fixes a system panic caused by a Windows95 or WindowsNT system sending an illegal length ping (ICMP)packet. • Fixes a kernel memory fault panic that occurs on SMP platforms when running the Unicenter product from Computer Associates in conjunction with Oracle software. • Fixes a problem in which broadcast packets are received by a daemon listening to a port that is using both the INP_RECVDSTADDR and SO_REUSEPORT socket options. The packets were not being delivered to the listening daemon. • Under certain conditions, a user on a remote host can cause a DIGITAL UNIX host to hang or panic. • Fixes a situation where an SMP machine acting as a network web server panics. The system will display panic strings such as the following: – "Unaligned kernel space access from kernel mode" – "Unaligned kernel space access from kernel mode" – "simple_lock: minimum spl violation" (when lockmode = 4) • Fix locking window exposed in sodequeue() when dozens of daemons (typically web servers) perform accept()'s on the same head socket. • Improves the performance of the network on a system being used as a web server. There are additional tuneable parameters included to be used by an experienced system administrator. • Fixes a problem in which the system panics when an interface is deleted. • System crashes with "Unaligned kernel space access from kernel mode" (Packetfilter unaligned access panic from ipintr).
Patch 319.00 OSF365-350390	**Patch:** Corrects cron Command Problem **State:** Existing 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.
Patch 321.00 OSF365-350392	**Patch:** Print Subsystem Corrections, lpr, lpq, lprm **State:** Supersedes patches OSF365-350172 (138.00), OSF365-350183 (145.00) This patch corrects the following: • Fixes a problem where the lpq command causes the program to crash (segmentation fault). • Print jobs created within a short timeframe, for example within the same second, were not sorted by print jobs and timestamps. • Print jobs cause existing jobs to be deleted from the queue whenever the number of print queue entries exceeded 1000.
Patch 322.00 OSF365-350413	**Patch:** audit_tool Command Correction **State:** New patch The audit_tool command hangs if the audit log contains pathnames that encounter boundary conditions.

Table 6–2: Summary of patches in Patch Kit-0004 (cont.)

Patch 323.00 OSF365-350395	**Patch:** vdump & vrestore Command Corrections **State:** Supersedes patches OSF365-350159 (132.00), OSF365-350201 (160.00), OSF365-350205 (163.00), OSF365-350389 (341.00), OSF365-350391 (320.00) This patch corrects the following: • Fixes a problem in which the vrestore command is unable to read data from a raw disk partition. • Fixes a problem where the vrestore program does not report failed exit status appropriately on incomplete or incorrect commands, corrupt or invalid saved sets, or file open failures. • Fixes a problem in which the vrestore command fails when running multiple iterations of the command in a script or from the command line. • Fix incorrect vdump file count message that shows up when vdump backs up a filesystem containing sockets. • User will receive the following error message if they attempt to restore a V4.0 dump on an older version of the OS: vrestore: Need vrestore V4.0 to restore contents; terminating
Patch 324.00 OSF365-350397	**Patch:** poll() System Call As A Timer. **State:** New patch Adds a mechanism to the poll() system call to allow it to be used as a timer.
Patch 325.00 OSF365-063	**Patch:** Reduce "NFS stale file handle" Messages Correction **State:** Supersedes patches OSF365-007 (7.00), OSF365-034 (34.00), OSF365-053 (299.00) This patch corrects the following: • Fix greatly reduces the number of "NFS stale file handle" messages logged to an NFS server system console. • Allows some third-party NFS v2 clients to experience a performance improvement. Candidate applications are ones that perform read/write operations to a memory mapped file over NFS. • A problem in which nfsportmon does not allow the root directory to be mounted from either a Solaris system or from an ULTRIX Version 4.2A system. • Fixes a problem where SUN NFS clients cannot write to files based on group membership. With this patch, a user who has group write permission on a file will be able to write to the file even when the directory containing the file does not have group write permission.

Table 6–2: Summary of patches in Patch Kit-0004 (cont.)

Patch 326.00 OSF365-350400	**Patch:** pax, cpio, tar Command Corrections **State:** Supersedes patches OSF365-350303 (221.00), OSF365-350333 (238.00) This patch corrects the following: • 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 pax's tar and cpio archive handling to allow filesizes greater than 4GB. • The tar(pax) command doesn't correctly handle sparse files, especially Oracle database files. Pre-allocated space is not replaced on restore.
Patch 327.00 OSF365-350418	**Patch:** awk/nawk Command Correction **State:** Supersedes patch OSF365-350056-1 (94.01) This patch corrects the following: • awk consumes memory until the machine swaps itself and core dumps with: write failed, file system is full Memory fault - core dumped • awk (nawk) doesn't always clear the previous value of the last field.
Patch 329.00 OSF365-350407	**Patch:** Device Driver Corrections **State:** Supersedes patch OSF365-350363 (286.00) This patch corrects the following: • Fixes a problem in which a system with an HSZ70 controller with a Q-Logic adapter or a KZPSA adapter may experience kernel memory faults during a failover and display a message similar to the following: panic (cpu 8): kernel memory fault cam_logger: CAM_ERROR entry too large to log! • A custom SCSI driver may return the error ENOMEM from its ccmn_open_unit() routine.
Patch 330.00 OSF365-350410	**Patch:** File System Incorrect User Type Correction **State:** New patch Fixes a problem that causes an AdvFS file system encapsulated under LSM to appear as a user type of "gen", rather than the correct type, "fsgen".

Table 6–2: Summary of patches in Patch Kit-0004 (cont.)

Patch 331.00 OSF365-350411	**Patch:** STREAMS ldtty, Kernel Panic Correction **State:** Supersedes patch OSF365-350150 (246.00), OSF365-350209 (250.00) This patch corrects the following: • Fixes a wide variety of system panics and other problems caused by random memory corruption. Problem noticed at sites hosting a lot of streams activity. • Pause or stall conditions of up to 30 seconds when an application calls the ldtty_close function in a STREAMS based implementation. After the pause or stall, the application resumes normal behavior with no other apparent side effects. • Successive reads wait for VTIME to expire regardless of VMIN setting assigned by ioctl.
Patch 332.00 OSF365-360109	**Patch:** "simple lock time limit exceeded" System Panic **State:** New patch Fixes a problem that occurs on SMP systems using LSM in which the system panics with a "simple lock time limit exceeded" message.
Patch 335.00 OSF365-066	**Patch:** System Crash With >1GB Of Memory **State:** Supersedes patches OSF365-028 (28.00), OSF365-038 (38.00) This patch corrects the following: • Fixes a problem where an AlphaServer 2100A system is shut down, using the "shutdown -r" command, the system will not reboot. • An AlphaServer 2100 or 2100A system with more than 1GB of memory will not boot when the dma window size is set in the sysconfigtab file. Typically the dma window size is set in the sysconfigtab file when Memory Channel is being used. • The UNIX kernel crashes during installation if the memory in the system exceeds 1GB. This has only been seen on AlphaServer 2100A class systems with greater than 1GB of memory.
Patch 336.00 OSF365-067	**Patch:** _zero() System Call Returns An Incorrect Value **State:** New patch Fixes a problem in which the io_zero() system call returns an incorrect value on an AlphaServer 1000.
Patch 345.00 OSF365-074	**Patch:** I/O Problems On AlphaStation 500 and 600 systems **State:** New patch Fixes several I/O problems in the kernel that occur on AlphaStation 500 and AlphaStation 600 systems. The problem causes these systems to hang or run with reduced performance.

Table 6–2: Summary of patches in Patch Kit-0004 (cont.)

Patch 346.00 OSF365-075	**Patch:** Various Kernel Corrections **State:** Supersedes patches OSF365-360010 (50.00), OSF365-360011 (51.00), OSF365-360012 (52.00), OSF365-360014 (54.00), OSF365-360015 (55.00), OSF365-360020 (58.00), OSF365-360023 (59.00), OSF365-017 (17.00), OSF365-360029 (64.00), OSF365-019 (19.00), OSF365-020-1 (20.01), OSF365-360039 (69.00), OSF365-360044 (72.00), OSF365-029-1 (29.01), OSF365-360046 (73.00), OSF365-360055 (80.00), OSF365-360056 (81.00), OSF365-360057 (82.00), OSF365-035-1 (35.01), OSF365-350082 (262.00), OSF365-360068 (88.00), OSF365-360070-1 (89.01), OSF365-360070-2 (89.02), OSF365-360076-1 (92.01), OSF365-009 (9.00), OSF365-350098 (106.00), OSF365-350113 (113.00), OSF365-010 (10.00), OSF365-013 (13.00), OSF365-015 (15.00), OSF365-350184 (146.00), OSF365-037 (37.00), OSF365-360085 (287.00), OSF365-050 (288.00), OSF365-050-1 (288.01), OSF365-360087 (289.00), OSF365-054 (304.00), OSF365-350372 (301.00), OSF365-360093 (303.00), OSF365-360101 (314.00), OSF365-350438 (339.00), OSF365-036 (36.00), OSF365-031 (31.00), OSF365-043 (43.00), OSF365-350309 (226.00), OSF365-005 (5.00), OSF365-027 (27.00), OSF365-051 (291.00), OSF365-350182 (144.00), OSF365-052 (292.00), OSF365-350405 (328.00), OSF365-068 (337.00), OSF365-350435 (352.00), OSF365-350438-1 (339.01), OSF365-073 (344.00), OSF365-350448 (356.00), OSF365-070 (342.00), OSF365-071 (343.00) This patch corrects the following: • Fixes a system crash when setting the date on SMP systems. • Fixes a system panic with the following panic string: "event_timeout: panic request" • Fixes an I/O queue corruption problem that occurs during normal shut down of SMP systems with AdvFS. • 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 error message: kernel memory fault • Provides general support for Version A11 KZPSA firmware. • 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. • 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.

Table 6–2: Summary of patches in Patch Kit-0004 (cont.)

Patch 346.00 continued	• Fixes panics that may occur on SMP systems. The following error message is displayed on the system: "simple_lock: time limit exceeded" • Non-retryable errors from an HSZ40 are not being logged in the system error log file. • Provides the following additional event logging by the SCSI/CAM disk driver: Additional Unit Attention messages, additional details for hard errors logged after unsuccessful I/O recovery attempts, and provides informational messages on the progress of recovery events. • Fixes various system problems: – System panic with: "xpt_callback: callback on freed CCB". – System panic with kernel memory fault while trying to remove an spo resource queue entry. – Logging following group of 3 errors every few minutes: spo_verify_adap_sanity, spo_misc_errors, spo_bus_reset when the system was under heavy load. – System then panicked with "simple_lock: time limit exceeded" after FS quiesced the bus on the HSZ40, powered off and disconnect tape drive for maintenance. – Infrequently, under heavy disk I/O loads, user data can be written to the wrong disk, resulting in data corruption. • A data corruption error which can occur on KZTSA SCSI adapters. This can result in data corruption on any tape drive connected to the KZTSA when large block (1 Meg or greater) transfers are performed. This data corruption has only been reported on odd block transfers. • Fixes a problem where a system panics with the following error message: "simple lock: time limit exceeded" This situation may occur during the creation of an Oracle database. • When HSZ50 hardware is installed, the system exhibits very slow performance. • Probe of isp fails intermittently during boot. • A number of problems have been fixed in the ISP driver. These include: "minimum spl violation" panics with lockmode=4, simple lock time limit exceeded panics, "CAM_ERROR entry too large" messages, and "Unable to restart Qlogic(LUN queue after abort)" panics.

Table 6–2: Summary of patches in Patch Kit-0004 (cont.)

Patch 346.00 continued	• A system can hang in "ss_process_timeouts", after binary.errlog entries: sim_err_sm Target went to command phase sim94_intr Illegal command panic: "xpt_callback: callback on freed CCB" • Eliminates panics that will occur when attempting to execute shell scripts on a filesystem mounted with the "noexec" option. • Fixes the corruption of core files produced by applications with 15 or more threads. • Fixes two system panics - no special situation that will cause these panics: – Fixes a panic that prints "kernel memory fault". – Fixes a panic that prints "pmap_dup: level3 PTE not valid". – Fixes a panic that prints "delete_pv_entry: mapping not in pv_list". • Fixes a problem with the exec() system function where 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 a problem that occurs on AlphaServer 8200 and 8400 systems when a processor fails to restart after a user halts the system by entering "Control-P Control-P" and then typing "continue" on the console. • 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. • Ladebug sessions may hang when debugging multithreaded applications. • Fixes system crash when setting the date for SMP systems. • Fixes a problem in which processes can hang waiting for a system call to table() to complete. • The system panics with "ipc_thread_init: reply port allocate" after an unsuccessful port allocation request. • Fixes the following: – AlphaServer 8200 systems do not correctly log 660 machine check errors. – AlphaServer 8200 systems do not provide enough information in the error log files to correctly diagnose 660 machine check errors. – On SMP machines, correctable processor error logging is inadvertently disabled at system boot up time.

Table 6–2: Summary of patches in Patch Kit-0004 (cont.)

Patch 346.00 continued	• In some situations the SWXCR controller may hang and I/Os won't complete. • Kernel panics with "zombie walks again" message. • Fixes System panic with "xcr_que_insert list corruption". • 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. • Enables the latest Informix KAIO functionality. The patch should be installed by Informix customers using the Informix 7.20.UC4 release. The Informix defect number 40041 regarding KAIO is fully addressed by this patch. • 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. • A system can crash with: panic: "pmap_remove_range: page wired" if certain kernel functions try to malloc more memory pages than allowed by the vm configuration parameter vm-vpagemax, which by default is set to 16384. • Fixes Ladebug process hangs when debugging user code. • A system will crash with " u_shm_oop_deallocate: reference count mismatch". • Multi-processor systems using the AdvFS file system, particularly systems also using AdvFS for the root and usr file systems, may experience intermittent freezing of interactive processes when the system has a moderate to heavy I/O load. The freezing of interactive processes may last from a few seconds to many minutes but will eventually return to normal. This problem may also occur on multi-processor systems using the NFS client or graphics sub-systems. • This patch is an upgrade/replacement for the FAA FDDI driver and fixes a halt/restart problem found in the old driver. The old driver could panic a system with a "simple_lock_fault violation" during a re-initialization. If a user binds a process to a processor and then halts that processor, the system may panic with a "simple lock owned" panic. • Fixes problems in tlb shootdown code: – Tlbshootdown requests could panic with timeouts because the other processor(s) do not respond to the interrupt. – The system may display invalid "tlb invalidate" messages. – There could be some memory data corruption or a memory fault. – Other processors in a cluster could have touched memory while it was being reset. – System panics with the error message: "tlb_shoot ack timeout".

Table 6–2: Summary of patches in Patch Kit-0004 (cont.)

Patch 346.00 continued	• Fix to allow clock to advance properly (wrap to next year) at end of year when system is powered down and to prevent clock from losing a day on each reboot during March of a leap year. • The system may experience a data corruption problem. This has been noted as causing a data corruption in the Oracle system table, but the corruption need not be limited to Oracle and could show up anywhere. • When executing with OSF PALcode revision 1.45, or greater, some floating point instructions fail. • A problem where a system may experience a panic with the panic string "pmap_remove_lev2: lev3 pte not valid", or the system may experience a data corruption problem. • Fix "panic: 'lock_write: interrupt level call'" in process group processing. • Fix memory and process state output from /proc PIOCPSINFO ioctl and SVE ps command. • Fixes "panic (cpu 0): kernel memory fault" from procfs_readdir()/uiomove() or procfs_lookup(). • Fortran programs using automatic arrays, C programs using alloca() functions, and other programs that allocate memory from the user's stack space, can experience segmentation violation errors. • System crashes with "kernel memory fault" when accessing proc file system. • User programs can end with a segmentation violation error when trying to allocate memory that grows in a downward direction. • This patch fixes the panic "thread_depress_wait" on multi-processor machines running multi-threaded applications. • Corrects an SMP/realtime-preemption race condition in the signal code that can allow a process stopped in sigsuspend to miss a signal wakeup and remaining block indefinitely. • Fixes a kernel crash that occurs when an asychronous I/O (aio) application calls the aio_suspend() function specifying the same aio control block multiple times.
Patch 347.00 OSF365-350419	**Patch:** FDDI Driver Corrections **State:** Supersedes patches OSF365-350145 (124.00), OSF365-350367 (290.00) This patch updates the FDDI driver to include these fixes: • Fixes a problem where after a hang the system crashes with the panic message: apecs_read_io_port. At that time, the only way to reboot the system is to switch it OFF then ON. • Upgrade/Replacement for the "FTA" FDDI driver and fixes a DMA Error which can occur with the older driver. • Major re-work of fta_reinitialize to fix stuck interface after halt. • Add code to display source and destination address on bad incoming packets (CRC, Illegal length, etc.). • Fixed the bumping of some DECnet counters so they could latch to their max values.

Table 6–2: Summary of patches in Patch Kit-0004 (cont.)

Patch 348.00 OSF365-350420	**Patch:** Security, mountd (SSRT0379U,SSRT0496U) **State:** Supersedes patches OSF365-350124 (116.00), OSF365-350177 (142.00), OSF365-350234 (181.00) This patch corrects the following: • A potential security vulnerability has been discovered in 'mountd', 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. • 'mountd' dies without logging the event in the daemon.log file and there is no core file. • Fixed a memory leak in 'mountd' which could cause 'mountd' to run out of virtual memory and terminate without issuing any error messages. • A potential security vulnerability has been discovered in 'mountd', where under certain circumstances users may gain unauthorized access. DIGITAL has corrected this potential vulnerability.
Patch 349.00 OSF365-350422	**Patch:** Kernel Panic, pty Correction **State:** Supersedes patches OSF365-350147 (126.00), OSF365-350174 (139.00), OSF365-350316 (230.00) This patch corrects the following: • Fixes the problem where applications running System V pseudoterminal slave pty can hang forever on open() system call. • Fixes a problem that causes the system to "assert_wait" panic with streams code on the stack. • Fixes a problem on a system where the ntalk daemons are hung. • The system becomes totally unresponsive every 2-5 days, not responding to terminals, the system console, or to pings. Added FIONREAD support for compatiblity with BSD.
Patch 350.00 OSF365-350423	**Patch:** doconfig Hang Correction **State:** New patch Fixes a problem the doconfig program hangs after being invoked by the uuxqt program.
Patch 351.00 OSF365-350431	**Patch:** date Command And >1999 Limitation Correction **State:** Supersedes patch OSF365-350255-1 (198.01) This patch corrects the following: • Fixes a problem in which the 'date' command is unable to set the date to January 1, 1970 00:00:00 GMT or February 29, 2000. • Enhancements to the date command for Year 2000 support.

Table 6–2: Summary of patches in Patch Kit-0004 (cont.)

Patch 353.00 OSF365-350440	**Patch:** Kernel Memory Fault Panic Corrections **State:** Supersedes patches OSF365-360027 (62.00), OSF365-360033 (67.00), OSF365-360033-1 (67.01),OSF365-350203 (161.00), OSF365-033 (33.00), OSF365-044-1 (44.01), OSF365-065 (334.00) This patch corrects the following: • 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 that occurs when running STREAMS. The system panics with a kernel memory fault in either osr_run() or osr_reopen(). • A problem that causes the system to panic with a kernel memory fault or "malloc_audit: guard space corruption" with osr_run as an entry in the stack. • Fixes a kernel memory fault panic on systems running System V applications or any user process compiled with the System V environment, even if System V is not loaded on the system. • Fixes panic in STREAMS code which is associated with high login/logout rates. • Fixes panic "simple_lock_time_violation". • The system panics with "kernel memory fault". The crash dump will show that the fault came from malloc or spec_reclaim. • A process can hang and a "kill -9" command will not kill it.
Patch 354.00 OSF365-350443	**Patch:** Linker Corrections **State:** Supersedes patches OSF365-350086 (100.00), OSF365-350120 (244.00), OSF365-350168 (135.00), OSF365-360049 (74.00), OSF365-360073 (91.00), OSF365-350337 (275.00) This patch corrects the following: • Fixes the following linker problems: – Hidden/export symbol wildcard problem – Assert getting generated with R_GPVALUE relocations – Improper Text segment alignment processing – Internal memory managment problem processing c++ program • 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. • Linker hangs (fails to complete execution).
Patch 355.00 OSF365-350445	**Patch:** Out Of Order Packets, Mem Leak Corrections **State:** Supersedes patch OSF365-350288 (212.00) This patch corrects the following: • Fixes a memory leak problem using the STREAMS Data Link Bridge (dlb) pseudodevice driver and could cause a "freeing free mbuf" panic when system memory is exhausted. • This patch corrects a problem with packets out of order experienced by some PATHWORKS Netbuei clients.

Table 6–2: Summary of patches in Patch Kit-0004 (cont.)

Patch 357.00	**Patch:** libc Corrections, Security (SSRT0359X)
OSF365-350449	**State:** Supersedes patches OSF365-350080 (99.00), OSF365-350108 (109.00), OSF365-350128 (117.00), OSF365-350133 (118.00), OSF365-360019 (57.00), OSF365-350153 (129.00), OSF365-350154 (130.00), OSF365-350217 (169.00), OSF365-350222 (172.00), OSF365-350236 (182.00), OSF365-350253 (196.00), OSF365-350279 (253.00), OSF365-360053 (78.00), OSF365-360082 (271.00), OSF365-360082-1 (340.00), OSF365-350412 (282.00) This patch corrects the following: • Fixes a problem where printing of a string with a specified precision could result in a segmentation fault. • 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 potential security vulnerability in BIND. • /sbin/shutdown takes too long if there are many open LAT lines. • 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. A problem that occurs after a user logs into a system with an SRV4-style LAT device. When the ttyslot function is called, the system fails to find the device and returns a value of zero, indicating an error in the ttyslot function. • Ensures that setlocale() does not call free() with a null pointer, which may crash an application that uses a third-party malloc package. • In some cases, sendmail generates a core dump when it receives an illegal command, after installing patch OSF365-350128. • A problem in the filename pattern-matching behavior of the find command when it includes the "?" metacharacter. The bug actually resides in fnmatch(), which is used by find. • Back out sprintf "%s" performance changes to fix "%*.*f" bug. • Multi-threaded applications run on DIGITAL UNIX V3.2[ABC] which use any of the get*_r() functions may dump core or produce incorrect results. • A potential security vulnerability has been discovered, where under certain circumstances users may gain unauthorized access. DIGITAL has corrected this potential vulnerability. • strncat() reads past end of source array. • Fixes multiple processes from adding duplicate ut_id lines in the utmp file with duplicate ut-id keys. • Several errors in the syslog entry written by the su program. • Fixes a problem with taso applications that set the malloc(3) __sbrk_override and __taso_mode tuning parameters to true. Under these circumstances, malloc(3) can return ENOMEM before all of the taso address space is allocated. • Fixes a memory leak problem associated with the strxfrm() and wcsxfrm() functions and some incorrect behavior in __do_replacement(), which is used by both strxfrm() and strcoll().

Table 6–2: Summary of patches in Patch Kit-0004 (cont.)

Patch 358.00 OSF365-350454	**Patch:** A Filesystem Cannot Be Unmounted. **State:** New patch A filesystem cannot be unmounted and the system displays a "Device busy" error message.
Patch 359.00 OSF365X-350037	**Patch:** Bookreader UID Handling Correction **State:** New patch 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.

Table 6–2: Summary of patches in Patch Kit-0004 (cont.)

Patch 360.00 OSF365X-350038	**Patch:** Corrects Memory Leak In The Motif Text Widgets **State:** Supersedes patch OSF365X-350035 (298.00) This patch corrects the following: • Motif Text widget is afflicted with a memory leak. A small amount of dynamic memory is lost each time the background colors in the widget are changed. • Motif applications may abort when you use the drag-and-drop feature.

Patch 362.00
OSF365-360125
	Patch: AdvFS Corrections
	State: Supersedes patches OSF365-360005 (49.00), OSF365-360013 (53.00), OSF365-360018 (56.00), OSF365-350123 (115.00), OSF365-350163 (134.00), OSF365-360028 (63.00), OSF365-360030 (65.00), OSF365-360041 (70.00), OSF365-360051 (76.00), OSF365-360061 (83.00), OSF365-350232 (179.00), OSF365-360067 (87.00), OSF365-360324 (235.00), OSF365-360031 (66.00), OSF365-360071 (90.00), OSF365-360088 (293.00), OSF365-360090 (295.00), OSF365-360105 (315.00), OSF365-360112 (361.00)
	This patch corrects the following:
	• Fixes a system panic when shutting down to single user mode using either one of the following commands when AdvFS is the root or usr filesystem:
	`# shutdown now`
	`# init s`
	• Fixes system panic with the following error message:
	`panic (cpu 0): kernel memory fault`
	• Fixes a problem with an NFS V3 mounted AdvFS file system where under heavy I/O load, data 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 system panic with the following error message:
	`AdvFS exception Module=26 line=1483`
	• Fixes to prevent the following two panics:
	– AdvFS Exception Module = 1, line = 1891
	– kernel memory fault
	– Idle time is reset on broadcast message when AdvFS is the root file system.
	– System panics with "kernel memory fault" in ubc_page_alloc().
	– This patch fixes a system panic with the message:
	"simple_lock: time limit exceeded".
	– This patch fixes a problem that occurs with the telnet and ftp commands. Telnet or ftp processes that are no longer in use, are left on the system indefinitely. When a user tries to log in, the login process hangs after displaying the last login message.

Patch 362.00 continued

- This patch fixes a problem in which a system using AdvFS can run out of metadata space when the AdvFS domain still has some free space available. The system will display error messages such as 'no space left on device'. The problem may occur on a heavily fragmented system with many small files, such as an Internet News server or Mail server.
- System panic with ADVFS EXCEPTION Module = 4, Line = 3541 "bs_unpinpg called with buffer not pinned".
- Advfs mmapped file data corruption when application fails to do msync(). The corruption is seen after rebooting the system when file changes were made via mmap(). Port of v32csuppportos-94-amilicia. Sreqeust is following bsubmit due to special dispensation from the gods of the build to get the bsubmit in before the build.
- Fixes a situation where an application that issues large read requests (each larger than 64 pages) can hang AdvFS or cause poor AdvFS performance. This patch fixes a problem in which an AdvFS system panics with the following message:

  "clear_buf: bufCnt = 0"

- Fixes kernel memory fault panic when mounting a crashed AdvFS file system.
- Fix "kernel memory fault" or "ADVFS EXCEPTION panic string: N1= -1027" panics during backup operations using AdvFS.
- System panics in AdvFS code when either:
  - ls command is run in the fileset mount directory (contains the .tags file).
  - msfsck is run at least twice and then the AdvFS fileset is unmounted.
- This patch fixes a problem in which a system that was upgraded to DIGITAL UNIX Version 3.2d1 and is running AdvFS, may not be able to mount its AdvFS multi- volume domain. Error messages will be displayed about incorrect sizes, volumes mounted read-only, or incorrect volume information.
- Fix for system panic "simple_lock_time_violation" with clearalias in stack trace.
- This patch fixes a problem in which the getrusage system call returns zero for the values of ru_inblock and ru_outblock on an AdvFS file system.
- Fixes NFS rpc.lockd "can't clear lock after crash of client" when AdvFS is being used.
- Fixes a problem in which an AdvFS system fails when attempting to create greater than 764490 files in a directory.

Patch 370.00
OSF365–350452

Patch: advfsstat -n" Causes A Core Dump

State: New patch

This patch fixes an AdvFS problem in which the "advfsstat -n" command causes a core dump. The system displays the following error message:

Memory fault(coredump)

7

Sample Patch Kit Installation

This chapter provides examples of sample installations.

7.1 Sample: Installation of Patches

```
Sample Installation Of Patches
# tar xpf DUV40BAS00003-19970425.tar
# patch_kit/dupatch
DIGITAL UNIX Patch Utility
==========================
(This dupatch session is logged in /var/adm/patch/log/session.log)

Main Menu:
---------

1) Patch Installation
2) Patch Deletion

3) Patch Documentation
4) Patch Tracking

5) Patch Baseline Analysis/Adjustment

h) Help on Command Line Interface

q) Quit

Enter your choice: 1

DIGITAL UNIX Patch Utility
==========================
(This dupatch session is logged in /var/adm/patch/log/session.log)

Patch Installation Menu:
------------------------

1) Pre-Installation Check ONLY
2) Check & Install (requires single-user mode)

b) Back to Main Menu

q)  Quit

Enter your choice: 2

 Gathering patch information...
    (depending upon the size of the patch kit, this may take a while)
    Notes for performing this operation. To end your input, enter a ".": : .

    - You have the option to make the patches reversible so you can
      revert the system to its state prior to the installation of a patch.

     - Reversibility is achieved by compressing and saving a copy of the
       files being replaced by the patches. These files would be restored
       to the system if you choose to remove a patch.

     - If you choose to make patches NON-reversible, then the system cannot
       be restored to the state prior to the installation of a patch; you
       will not be able to remove the patches later.

     - This patch kit may force a small set of patches to be reversible to
       ensure your upgrades to future versions of DIGITAL UNIX are successful.
       The Patch Utility will make those patches reversible automatically.

       Refer to the Release Notes / Installation Instructions provided with
       this patch kit.

  Do you want the patches to be reversible? [y]: y
```

```
   - By default, the backup copies of the installed patches will be saved
     in "/var/adm/patch/backup".

   - If you have limited space in /var, you may want to make the backup
     directory the mount point for a separate disk partition, an NFS
     mounted directory, or a symbolic link to another file system.

    - You must ensure the backup directory is configured the same way during
      any patch removal operations.

Your current setup of "/var/adm/patch/backup" is:

        * A plain directory (not a mount point or a symbolic link)
Do you want to proceed with the installation with this setup? [y/n]: y

The subsets listed below are optional:

     There may be more optional subsets than can be presented on a single
     screen. If this is the case, you can choose subsets screen by screen
     or all at once on the last screen. All of the choices you make will
     be collected for your confirmation before any subsets are installed.

 - Commands, Shells, & Utility Patches:
     1) V4.0B Patch 0010.00 - Patch: dump and rdump Command Corrections

     2) V4.0B Patch 0017.00 - Patch: ksh Correction
     3) V4.0B Patch 0019.00 - Patch: quota Command Correction

 - Filesystem Patches:
     4) V4.0B Patch 0007.00 - Patch: Filesystem And vmstat Command Corrections

 - I/O Device Handling Patches:
     5) V4.0B Patch 0003.00 - Patch: PCXAL, LK411, And Similar Keyboards

     6) V4.0B Patch 0006.00 - Patch: Prevents Delivery Of Data In Subsequent Str
     7) V4.0B Patch 0009.00 - Patch: ddr_config Corrections

--- MORE TO FOLLOW ---

Enter your choices or press RETURN to display the next screen.

Choices (for example, 1 2 4-6):

 - Library Patches:
    8) V4.0B Patch 0012.00 - Patch: libm Corrections
    9) V4.0B Patch 0016.00 - Patch: auth_for_terminal() Segmentation Fault Corr

   10) V4.0B Patch 0018.00 - Patch: libc Corrections
   11) V4.0B Patch 0024.00 - Patch: Threads Corrections

 - Memory Handling Patches:
   12) V4.0B Patch 0022.00 - Patch: Virtual Memory Corrections

 - Terminal Handling Patches:
   13) V4.0B Patch 0013.00 - Patch: Remote Login With c-list Type ttys

 - X11 Patches:
   14) V4.0B Patch 0004.00 - Patch: Change Cursor Reporting In The Workstation

--- MORE TO FOLLOW ---

Enter your choices or press RETURN to display the next screen.

Choices (for example, 1 2 4-6):
Or you may choose one of the following options:

   15) ALL of the above
   16) CANCEL selections and redisplay menus
   17) EXIT without installing any subsets

Enter your choices or press RETURN to redisplay menus.

Choices (for example, 1 2 4-6): 15

You are installing the following optional subsets:

- Commands, Shells, & Utility Patches:
       V4.0B Patch 0010.00 - Patch: dump and rdump Command Corrections

       V4.0B Patch 0017.00 - Patch: ksh Correction
```

```
        V4.0B Patch 0019.00 - Patch: quota Command Correction

 - Filesystem Patches:
        V4.0B Patch 0007.00 - Patch: Filesystem And vmstat Command Corrections

 - I/O Device Handling Patches:
        V4.0B Patch 0003.00 - Patch: PCXAL, LK411, And Similar Keyboards

        V4.0B Patch 0006.00 - Patch: Prevents Delivery Of Data In Subsequent Str
        V4.0B Patch 0009.00 - Patch: ddr_config Corrections

  - Library Patches:
        V4.0B Patch 0012.00 - Patch: libm Corrections
        V4.0B Patch 0016.00 - Patch: auth_for_terminal() Segmentation Fault Corr

         V4.0B Patch 0018.00 - Patch: libc Corrections
         V4.0B Patch 0024.00 - Patch: Threads Corrections

 Press RETURN to display the next screen:

  - Memory Handling Patches:
        V4.0B Patch 0022.00 - Patch: Virtual Memory Corrections

  - Terminal Handling Patches:
        V4.0B Patch 0013.00 - Patch: Remote Login With c-list Type ttys

  - X11 Patches:
        V4.0B Patch 0004.00 - Patch: Change Cursor Reporting In The Workstation

 Is this correct? (y/n): y

 Checking patch prerequisites and patch file applicability...
 (depending upon the number of patches you select, this may take a while)
 ------------------------------------------------------------------------------

Problem installing:
        "V4.0B Patch 0010.00 - Patch: dump and rdump Command Corrections" -

         Can not identify the origin of ./sbin/dump.

         This patch will not be installed.
------------------------------------------------------------------------------

         * Following patch(es) failed in prerequisite/file applicability check:

            "V4.0B Patch 0010.00 - Patch: dump and rdump Command Corrections"

 Select the action you'd like to take:
    1)  proceed with the patches that passed the check
    2)  select patches again
    3)  go back to the Patch Installation Menu

 Enter your choice: 1

 Checking patch prerequisites once more...
  (depending upon the number of patches you select, this may take a while)

 ************************* CAUTION ************************************
         Interruption of this phase of the operation will corrupt your
         operating system software and compromise the patch database
         integrity.

         DO NOT Ctrl/C, power off your system, or in any other way
         interrupt the patch operation. The patch operation is complete
         when you are returned to the Patch Utility menus.
 **********************************************************************

 Checking file system space required to install specified subsets:

 13 subset(s) will be installed.  Loading 1 of 13 subset(s)....

 Patch: PCXAL, LK411, And Similar Keyboards
   Copying from /usr/patch_kit/patch_kit/kit (disk)
   Verifying

 Loading 2 of 13 subset(s)....

Patch: Change Cursor Reporting In The Workstation Driver
   Copying from /usr/patch_kit/patch_kit/kit (disk)
   Verifying
```

```
Loading 3 of 13 subset(s)....

Patch: ddr_config Corrections
  Copying from /usr/patch_kit/patch_kit/kit (disk)
  Verifying

Loading 4 of 13 subset(s)....

Patch: libm Corrections
  Copying from /usr/patch_kit/patch_kit/kit (disk)
  Verifying

Loading 5 of 13 subset(s)....

Patch: Remote Login With c-list Type ttys
  Copying from /usr/patch_kit/patch_kit/kit (disk)
  Verifying

Loading 6 of 13 subset(s)....

Patch: auth_for_terminal() Segmentation Fault Correction
  Copying from /usr/patch_kit/patch_kit/kit (disk)
  Verifying

Loading 7 of 13 subset(s)....

Patch: ksh Correction
  Copying from /usr/patch_kit/patch_kit/kit (disk)
  Verifying

Loading 8 of 13 subset(s)....

Patch: libc Corrections
  Copying from /usr/patch_kit/patch_kit/kit (disk)
  Verifying

Loading 9 of 13 subset(s)....

Patch: quota Command Correction
  Copying from /usr/patch_kit/patch_kit/kit (disk)
  Verifying

Loading 10 of 13 subset(s)....

Patch: Virtual Memory Corrections
  Copying from /usr/patch_kit/patch_kit/kit (disk)
  Verifying

Loading 11 of 13 subset(s)....

Patch: Threads Corrections
  Copying from /usr/patch_kit/patch_kit/kit (disk)
  Verifying

Loading 12 of 13 subset(s)....

Patch: Prevents Delivery Of Data In Subsequent Streams Msgs
  Copying from /usr/patch_kit/patch_kit/kit (disk)
  Verifying

Loading 13 of 13 subset(s)....
Patch: Filesystem And vmstat Command Corrections
  Copying from /usr/patch_kit/patch_kit/kit (disk)
  Verifying

13 of 13 subset(s) installed successfully.

Configuring "Patch: PCXAL, LK411, And Similar Keyboards" (OSFPAT00000300410)

Configuring "Patch: Change Cursor Reporting In The Workstation Driver" (OSFPAT00000400410)

Configuring "Patch: ddr_config Corrections " (OSFPAT00000900410)

Configuring "Patch: libm Corrections " (OSFPAT00001200410)

Configuring "Patch: Remote Login With c-list Type ttys" (OSFPAT00001300410)

Configuring "Patch: auth_for_terminal() Segmentation Fault Correction" (OSFPAT00001600410)

Configuring "Patch: ksh Correction " (OSFPAT00001700410)
```

```
  Configuring "Patch: libc Corrections " (OSFPAT00001800410)

  Configuring "Patch: quota Command Correction " (OSFPAT00001900410)

  Configuring "Patch: Virtual Memory Corrections " (OSFPAT00002200410)

  Configuring "Patch: Threads Corrections " (OSFPAT00002400410)

  Configuring "Patch: Prevents Delivery Of Data In Subsequent Streams Msgs" (OSFPAT00000600410)

  Configuring "Patch: Filesystem And vmstat Command Corrections " (OSFPAT00000700410)

          * A kernel rebuild is required for the successfully installed
           patch(es).

DIGITAL UNIX Patch Utility
==========================
(This dupatch session is logged in /var/adm/patch/log/session.log)

Patch Installation Menu:
------------------------

1) Pre-Installation Check ONLY
2) Check & Install (requires single-user mode)

b) Back to Main Menu
q) Quit

Enter your choice: b
```

7.2 Sample: Patch Documentation Viewing

```
# dupatch

DIGITAL UNIX Patch Utility
==========================
(This dupatch session is logged in /var/adm/patch/log/session.log)

Main Menu:
----------

1) Patch Installation
2) Patch Deletion

3) Patch Documentation
4) Patch Tracking

5) Patch Baseline Analysis/Adjustment

h) Help on Command Line Interface

q) Quit

Enter your choice: 3

DIGITAL UNIX Patch Utility
==========================
(This dupatch session is logged in /var/adm/patch/log/session.log)

Patch Documentation Menu:
-------------------------

1) View patch abstract of installed patches on your system
2) View patch abstract of patches on the patch kit

3) View patch README of installed patches on your system
4) View patch README of patches on the patch kit

5) View all patch abstract on your system
6) View all patch README on your system

b) Back to Main Menu
q) Quit

Enter your choice: 2

      There may be more subsets than can be presented on a single
```

```
    screen. If this is the case, you can choose subsets screen by screen
    or all at once on the last screen. All of the choices you make will
    be collected for your confirmation before any subsets are examined.

 - Commands, Shells, & Utility Patches:
     1) V4.0B Patch 0010.00 - Patch: dump and rdump Command Corrections
     2) V4.0B Patch 0017.00 - Patch: ksh Correction
     3) V4.0B Patch 0019.00 - Patch: quota Command Correction

 - Filesystem Patches:
     4) V4.0B Patch 0007.00 - Patch: Filesystem And vmstat Command Corrections

 - I/O Device Handling Patches:
     5) V4.0B Patch 0003.00 - Patch: PCXAL, LK411, And Similar Keyboards
     6) V4.0B Patch 0006.00 - Patch: Prevents Delivery Of Data In Subsequent Str

     7) V4.0B Patch 0009.00 - Patch: ddr_config Corrections

Enter your choices or press RETURN to display the next screen.

Choices (for example, 1 2 4-6): 1-2

 - Library Patches:
    8) V4.0B Patch 0012.00 - Patch: libm Corrections

    9) V4.0B Patch 0016.00 - Patch: auth_for_terminal() Segmentation Fault Corr
   10) V4.0B Patch 0018.00 - Patch: libc Corrections

   11) V4.0B Patch 0024.00 - Patch: Threads Corrections

 - Memory Handling Patches:
   12) V4.0B Patch 0022.00 - Patch: Virtual Memory Corrections

 - Terminal Handling Patches:
   13) V4.0B Patch 0013.00 - Patch: Remote Login With c-list Type ttys

 - X11 Patches:
   14) V4.0B Patch 0004.00 - Patch: Change Cursor Reporting In The Workstation

Add to your choices or press RETURN to display the next screen.

Choices (for example, 1 2 4-6):  1-2

The following choices override your previous selections:
   15) ALL of the above
   16) CANCEL selections and redisplay menus
   17) EXIT without examining any subsets

Add to your choices, choose an overriding action or
press RETURN to confirm previous selections.

Choices (for example, 1 2 4-6):  1-2
You are examining the following subsets:

 - Commands, Shells, & Utility Patches:
       V4.0B Patch 0010.00 - Patch: dump and rdump Command Corrections
       V4.0B Patch 0017.00 - Patch: ksh Correction

Is this correct? (y/n): y

=============================================================================
* V4.0B Patch 0010.00 - Patch: dump and rdump Command Corrections:

This patch 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.

=============================================================================
* V4.0B Patch 0017.00 - Patch: ksh Correction:

This patch 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.

Press RETURN to get back to the Patch Documentation Menu.

DIGITAL UNIX Patch Utility
```

```
==========================
      (This dupatch session is logged in /var/adm/patch/log/session.log)

  Patch Documentation Menu:
  -------------------------

  1) View patch abstract of installed patches on your system
  2) View patch abstract of patches on the patch kit

  3) View patch README of installed patches on your system
  4) View patch README of patches on the patch kit

  5) View all patch abstract on your system
  6) View all patch README on your system

  b) Back to Main Menu
  q) Quit

  Enter your choice: b
```

7.3 Sample: Setting System Baseline for Patch Kits

```
DIGITAL UNIX Patch Utility
==========================
(This dupatch session is logged in /var/adm/patch/log/session.log)

 Main Menu:
 ----------

1) Patch Installation
2) Patch Deletion

3) Patch Documentation
4) Patch Tracking

5) Patch Baseline Analysis/Adjustment

h) Help on Command Line Interface

q) Quit

Enter your choice: 5

  Patch Baseline Analysis and Adjustment
  ======================================

  This section of the patch management utility does not actually install
  patches. It is an enabler and need only be used to baseline your
  system for routine use of setld-based patch kits. It is recommended that
  you read the release notes
  accompanying this kit, prior to continuing.

  It is specifically designed to provide continuity from an environment with
  manually installed operating system patches to one that can be managed
  using the standard 'setld' installation technology.

  This baselining is broken into phases that assess and report the state of
  your operating system files. It will only make changes to your system with
  your confirmation.

      Phase 1 - System Evaluation

         Where possible, this phase determines the origin of changed operating
         system files and detects formally released official patches that were
         manually installed.

      Phase 2 - Report patches with layered product conflicts

         Some layered products ship operating system files. If any such files
         exist on your system, they will show up during this phase.  You can
         NOT install patches that intersect with a layered product as it would
         corrupt the layered product operation.

      Phase 3 - Create installation records for manually installed patches

        During this phase, you will be shown a list of patches that match
        the operating system files on your system. You will be offered an
        opportunity to mark these patches as 'installed' on your system.
```

```
        This involves copying valid 'setld' database information to your
        system.

      Phase 4 - Report changed system files not included in the patch kit

        This phase provides information to help you make choices later in
        this process. The files which appear in this phase are changed on
        your system but their origin cannot be determined.  They are also
        not part of the patch kit under evaluation.  You will want to
        consider this information when you later make decisions in phase 5.

      Phase 5 - Enable patches with file conflicts or missing system files

        This phase allows you to enable subsequent installation of patches
        whose inventory does not match the installed system.  This occurs
        when, 1) system files change and the origin of that change cannot
        be deteremined, 2) the original file to be patched is missing from
        the system.

        It is recommended that you do not enable the installation of these
        patches, if any, until you have tracked down the origin of the
        files that are in conflict, or you may compromise the integrity of
        your operating system.

        To assist you in this effort, the file list for the entire patch
        with the known information will be displayed. You may run through
        this phase to get the analysis without enabling the installation
        of any of the listed patches.

        It is recommended that you backup your operating system prior to
        the actual patch installation.

      Do you want to proceed with the analysis and adjustment? [y/n]: y

      - This Patch Baseline Analysis/Adjustment session is logged in:
                /var/adm/patch/log/baseline.log

      - Previous baseline.log saved to baseline.bak

 Phase 1 - System Evaluation
 ===========================

    This evaluation compares the contents of your patch kit to the origin.

    The amount of time needed to complete this phase can vary greatly
    depending on the size of the patch kit, the version of the Operating
    System, and the performance of the system.

     * system evaluation completed.
      ----------------------------

    Press RETURN to proceed to the next phase.

 Phase 2 - Report patches with layered product conflicts
=========================================================

    Some layered products replace files delivered in the original Operating
    System inventory.  The Patch Utility will block installation of these
    patches since that could compromise the integrity of the layered products.

    * no layered product conflicts detected.
      ------------------------------------

     Press RETURN to proceed to the next phase.

 Phase 3 - Create installation records for manually installed patches
======================================================================

    You can choose to copy valid installation records to your system for
    the following patches, if any.  This will allow future management and
    reporting for patches to your operating system.

    Creating installation records is intended to establish a baseline to
    which future patches might be applied.  Future patch removal may
    only ever occur to this baseline.

    * no manually installed patches detected.
     ----------------------------------------

    Press RETURN to proceed to the next phase.
```

```
 Phase 4 - Report changed system files not included in the patch kit
=====================================================================

    The following files, if any, have been changed since the original
    installation in a way which cannot be determined

    Because they are not part of the patch kit, they may not interact
    properly with the patches in the kit.  The list should be considered
    carefully when making decisions to enable installation of certain
    patches in Phase 5.

    * no changed system files not included in the patch kit detected.
    ----------------------------------------------------------------

     Press RETURN to proceed to the next phase.

 Phase 5 - Enable patches with file conflicts or missing system files
=====================================================================

    You will be shown a list of patches, if any, and their files.
    Patches show up during this phase because all or part of their
    inventory contain changed operating system files with unknown origin
    or the files to be replaced are missing on your system.

    After reviewing this section, you can elect to enable the installation
    of these patches using a standard selection menu. Enabling a patch
    means that the patch file applicability checks, done during patch
    installation, will be overridden if you later choose to install that
    patch through the installation section of dupatch.

    It is recommended that you understand the origin of the listed files
    before enabling a patch for installation.

    Press RETURN to see the list of patches.

    * list of patches with changed files of unknown origin or missing files:
    ------------------------------------------------------------------------

      V4.0B Patch 0010.00 - Patch: dump and rdump Command Corrections
           - Changed files with unknown origin are:
               ./sbin/dump
          - Other file(s) within this patch, with their origin (identified
            through checksum match) listed in terms of subset identifier(s),
            if any, are:
               ./usr/lib/nls/msg/en_US.ISO8859-1/dump.cat
                     OSFHWBASE410
               ./usr/sbin/dump
                        OSFHWBASE410
               ./usr/sbin/rdump
                        OSFCLINET410

 Do you want to enable the installation of any of these patches? [y/n]: n

 * Baseline Analysis/Adjustment process completed.
  ==============================================

 Press RETURN to get back to the Main Menu.

 DIGITAL UNIX Patch Utility
 ==========================
 (This dupatch session is logged in /var/adm/patch/log/session.log)

 Main Menu:
 -----------

 1) Patch Installation
 2) Patch Deletion

 3) Patch Documentation
 4) Patch Tracking

 5) Patch Baseline Analysis/Adjustment

 h) Help on Command Line Interface

 q) Quit

 Enter your choice: q
```