DIGITAL UNIX

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

April 1998

Product Version: DIGITAL UNIX Version 3.2C

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

1 Introduction

2 Features and Restrictions

3 Release Notes

4 Installation Instructions

5 DIGITAL UNIX System Upgrade Information

6 Summary of Patches

7 Sample Patch Kit Installation

Tables

About This Manual

This manual contains information specific to Patch Kit-0004 for the DIGITAL UNIX Version 3.2C 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 ~36.5 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 ~37.2 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 ~640 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 3.2C System

If you are upgrading your patched Version 3.2C 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 3.2D/E-1, Version 3.2D/E-2, 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:

  - 116.00 (OSF350-116)
  - 190.00 (OSF350–190)
  - 221.00 (OSF350–221)
  - 241.00 (OSF350–241)
  - 274.00 (OSF350–274)
  - 282.00 (OSF350–282)
  - 325.00 (OSF350X-015)

- 334.00 (OSF350–348B)
- 337.00 (OSF350–298)
- 340.00 (OSF350–302)
- 372.00 (OSF350–336)
- 400.00 (OSF350–374)
- 409.00 (OSF350–382)
- 424.00 (OSF350–404)
- 411.00 (OSF350–384)
- 415.00 (OSF350–348C)
- 416.00 (OSF350–395)
- 417.00 (OSF350–462)
- 444.00 (OSF350–432)
- 450.00 (OSF350–444)
- 454.00 (OSF350–449)
- 458.00 (OSF350–465)

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 3.2C. This list will be updated and managed for each patch kit.

3.3 Special Instructions for Patch 417.00 (Granularity Hints)

You will need to reset the date and time following the initial system reboot required to use the newly built kernel that enables Patch 417.00. This is only required on the initial system reboot.

3.4 Special Instructions for Patches 417.00 and 458.00 (AdvFS Consolidated Patch)

If you install Patch 417.00 without Patch 458.00 (for example, because you aren’t using AdvFS) and then start using AdvFS without first installing Patch 458.00, your memory buffer cache may be misconfigured. This will not prevent configuration or single-user booting of the system, but in specific cases may cause a degradation in performance.

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 3.2C 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 213.00	Superseded by Patch 213.01
Patch 375.00	Superseded by Patches 458.00, 440.00, 407.00
Patch 387.00	Superseded by Patch 400.00
Patch 352.00	Superseded by Patch 409.00
Patch 369.00	Superseded by Patch 420.00
Patch 244.00	Superseded by Patch 424.00
Patches 349.00, 347,00, 385.00	Superseded by Patches 417.00, 437.00, 457.00, 453.00, 448.00, 447.00, 349.01, 445.00, 442.00, 441.00, 427.00, 425.00, 423.00
Patch 381.00	Superseded by Patch 426.00
Patch 209.00	Superseded by Patch 429.00
Patch 348.00	Superseded by Patches 454.00, 430.00, 419.00
Patch 56.00	Superseded by Patch 433.00
Patch 386.00	Superseded by Patch 434.00
Patch 234.00	Superseded by Patch 436.00
Patch 354.00	Superseded by Patch 438.00
Patch 255.00	Superseded by Patch 443.00
Patch 373.00	Superseded by Patch 449.00
Patch 262.00	Superseded by Patch 450.00
Patch 288.00	Superseded by Patch 451.00
Patch 311.00	Superseded by Patch 435.00
Patch 398.00	Superseded by Patch 350.00

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 4.00 OSF350-004	**Patch:** Root Logout Auditing, Restrict setsysinfo Access **State:** Existing This patch corrects the following: • Root logouts are not being audited when auditing of logouts was enabled. • Calls to setsysinfo(SSI_ULIMIT) were not restricted to superuser (root).
Patch 10.00 OSF350-010	**Patch:** FP Correction For cmptun Instruction **State:** Existing cmptun instruction can return TRUE when no NaN is present.
Patch 15.00 OSF350-015	**Patch:** chmod Corrections **State:** Existing chmod -R will cause files which are targets of symbolic links to receive incorrect permissions.
Patch 17.00 OSF350-017	**Patch:** vm_object_free Panic Correction **State:** Existing System panics with the message: vm_object_free: res count > 1
Patch 18.00 OSF350-018	**Patch:** yacc Command Corrections **State:** Existing YACC fails with a Memory fault when used on large grammar file.
Patch 19.00 OSF350-019	**Patch:** Common Agent (snmp) Corrections **State:** Existing This patch corrects the following: • snmp_pe core dumps when receiving unusual SNMP packets. • snmp_pe does not support the "no_auth_trap" directive in snmp_pe.conf. • When running the snmpCollect daemon of Polycenter Netview 4.1, but could occur when any random SNMP application formats packets unusually (not necessarily improperly).
Patch 34.00 OSF350-034	**Patch:** PXG Family 2D Graphics Card Panic Correction **State:** Existing PXG Family 2D Graphics Card Panic Correction: The system panics during the initialization of the X server (which usually occurs at the end of system startup when xdm is started).
Patch 39.00 OSF350-039	**Patch:** I/O Device Handling Patches **State:** Existing Using high-speed modems with LAT: application may fail because tty speed is set to 0.
Patch 40.00 OSF350-040	**Patch:** LAT Misses Data on Delayed TTY Close Correction **State:** Existing An application that opens a LAT tty only once should be allowed to issue writes before the connection is fully established.
Patch 42.00 OSF350-042	**Patch:** User Level Action Panics System Correction **State:** Existing Any user can cause a system panic by doing a read or ioctl on /dev/streams/dlpi (i.e., the command "file /dev/streams/dlpi").

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

Patch 48.00 OSF350-048	**Patch:** Security, MAKEDEV **State:** Existing A potential security vulnerability has been discovered, where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability.
Patch 53.00 OSF350-053	**Patch:** LSM rootdg Configuration Correction **State:** Existing Fixes a problem that only occurs when the configuration database in the rootdg diskgroup has records that will not fit in 512 sectors.
Patch 57.00 OSF350-057	**Patch:** KSPSA Driver Panic Correction **State:** Existing KSPSA driver panics with a "simple lock timeout" message. This can happen in ASE environments that have intermittent SCSI bus problems.
Patch 61.00 OSF350-061	**Patch:** Security, rdist (SSRT0329U) **State:** Existing A potential security vulnerability has been discovered, where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability.
Patch 66.00 OSF350-066	**Patch:** Panic If RAID Set Disk Is Mislabeled (rz) **State:** Existing The system can panic when a disk is in a RAID set and is mislabelled.
Patch 69.00 OSF350-069	**Patch:** Memory Corruption Correction **State:** Existing When illegal user arguments are passed to the semop() system call, such that exactly none of the requested operations work, the system call code continues in a path that corrupts memory by depositing a PID number in areas beyond the semaphore structures allocated memory. When this occurs, the 16-byte elements in kmembuckets[0] are the target of the corruption.
Patch 71.00 OSF350-071	**Patch:** PCI (pciaerror) System Panic Correction **State:** Supersedes patch OSF350-033 This patch corrrects the following: • DEC 8200 and 8400 systems with PCI configurations panic with the "pciaerror" message string.
Patch 73.00 OSF350-073	**Patch:** BOOTP Server Daemon Correction **State:** Existing The bootp daemon appends a null character to file names in its responses.
Patch 76.00 OSF350-076	**Patch:** Support For 32 SCSI Buses In scu Command **State:** Existing The /sbin/scu command is currently limited to supporting 16 SCSI buses numbered from 0 to 15.
Patch 89.00 OSF350-089	**Patch:** tftpd Server Correction **State:** Existing Attempting to tftpd to an aliased interface will give "ICMP Destination unreachable" messages when multiple read requests are required to transfer data.

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

Patch 96.00 OSF350-096	**Patch:** acctcms Command Hash Table Overflow Correction **State:** Existing Fixes acctcms hash table overflow error.
Patch 97.00 OSF350-097	**Patch:** FreePort Express Binary Translator Correction **State:** Existing Program translated with FreePort Express (SunOS –> DIGITAL UNIX) binary translator does not run correctly.
Patch 100.00 OSF350-100	**Patch:** RAID Set Dump Device, No Crash Dump After Panic **State:** Existing A system which has a RAID set for a dump device will experience the following problem: the system will not save the crash dump after a panic.
Patch 102.00 OSF350-102	**Patch:** Process Stops Responding To Signals **State:** Existing Programs using libexc.a suffer corrupted signal masks.
Patch 109.00 OSF350-109	**Patch:** NFS File Server w/ Non-DIGITAL UNIX Client Correction **State:** Existing Fixes file corruption on a DIGITAL UNIX NFS fileserver serving a non-DIGITAL UNIX client. The problem was caused by client XID reuse and was originally seen when the only nfs client was an OS/2 PC.
Patch 111.00 OSF350-111	**Patch:** tip Uses ~45 Percent Of CPU Time **State:** Existing Running tip used approximately 45% of CPU time, which was excessive.
Patch 112.00 OSF350-112	**Patch:** Security, lattelnet (Configuration Specific) **State:** Existing Users could use lattelnet to invoke a subshell, a potential security issue in some installations.

Patch 114.00
OSF350-114
	Patch: Assembler Correction
	State: Existing
	Fix 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 115.00 OSF350-115	**Patch:** ATM IP Correction **State:** Existing Corrects a card lockup problem using the ATM IP convergence module.
Patch 116.00 OSF350-116	**Patch:** Loadable PCI Driver With >1 PCI Bus **State:** Existing Systems utilizing loadable PCI device driver support will fail to configure loadable PCI device drivers when more than one PCI bus exists in a system.
Patch 117.00 OSF350-117	**Patch:** SCSI Bus Hang Using KZMSA & HSZ40 **State:** Existing A system hang or a SCSI bus hang will be experienced, when using KZMSA and HSZ40s.

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

Patch 121.00 OSF350-121	**Patch:** VME Bus Adaptor Corrections **State:** Existing This patch corrects the following: • On DIGITAL Alpha VME 2100 Systems with EV4.5 or EV5 processors with the embedded VIP/VIC64 VME bus adapter, the system may crash. • System panics with a machine check, a VME adapter error occurs with an indication that a PCI Target abort occurred, or data corruption occurs transfering data between VME devices and system memory. • Master Block Transfer hardware DMA performance is poor on the embedded VIP/VIC64 VME bus of DIGITAL Alpha VME 2100 and AXPVME systems.
Patch 130.00 OSF350-130	**Patch:** STRLOG Concatenation Of Sequential Outputs **State:** Existing The strace command gets STREAMS event trace messages from STREAMS drivers and modules via the STREAMS log driver (strlog). STRLOG had a bug that caused concatenation of sequential outputs.
Patch 139.00 OSF350-139	**Patch:** VM Fault Handling In UFS **State:** Supersedes patch OSF350-054 (54.00) This patch corrects the following: • Large DB application hangs in uninterruptable state. • System panic with "ufs_getapage: allocation failed" message.
Patch 143.00 OSF350-143	**Patch:** Runtime Linker and Loader Correction **State:** Existing A call-share executable with a text, data or bss region greater than 4 gbytes the application will segment fault. As a workaround you can build your application non-share.
Patch 144.00 OSF350-144	**Patch:** DIGITAL Peer Server & Token Ring Setup Wrong **State:** Existing After installing and configuring DIGITAL Peer Server version 1.3, EC01, token ring source routing tables may not be built correctly. If you have multiple token ring interfaces, additional interfaces will not initialize and links between remote stations cannot be established.
Patch 149.00 OSF350-149	**Patch:** Long Copy Of >10MB Files (PW-OSF Server/WfW Client) **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 152.00 OSF350-152	**Patch:** Security (SSRT0376X) **State:** Existing A potential security vulnerability has been discovered, where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability.
Patch 155.00 OSF350-155	**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 156.00 OSF350-156	**Patch:** pnvram Correction **State:** Existing Corrects system panic with the message "pnvram_write: Timed-out DMA".
Patch 161.00 OSF350-161	**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 167.00 OSF350-167	**Patch:** ioctl() Using The TIOCM_RI Mask Always Fails **State:** Existing Fixes a problem where a call to ioctl() using the TIOCM_RI mask always fails.
Patch 169.00 OSF350-169	**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 176.00 OSF350-176	**Patch:** find Command Returns Invalid Sts Code **State:** Existing Fixes a problem where the find command returns a invalid status code upon encountering a file in an "ffm" set.
Patch 185.00 OSF350-185	**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 186.00 OSF350-186	**Patch:** netsetup ioctl: Invalid Argument Error **State:** Existing After running "strsetup -i -f" /dev/streams/kinfo and /dev/streams/strkinfo can have the same major and minor numbers. This causes "netsetup" to report "ioctl: invalid argument" errors.
Patch 190.00 OSF350-190	**Patch:** sysfs: Function Not implemented (add ffm & nfsv3) **State:** Existing Adds support for file system ids ffm and nfsv3.
Patch 191.00 OSF350-191	**Patch:** Remote Execution Server (rexecd) Correction **State:** Existing Fixes the condition that results when there is no default shell in the password file causing rexecd to fail.
Patch 198.00 OSF350-198	**Patch:** rcp Command Correction (Handling >2GB File) **State:** Existing 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 200.01 OSF350-200-1	**Patch:** df Command Correction **State:** Supersedes patch OSF350-200 (200.00) This patch corrects the following: • Fixes a problem in which the output from the df command displays incorrectly formatted columns.
Patch 206.00 OSF350-206	**Patch:** ping -ff Segmentation Fault **State:** Existing "ping -p ff" results in a segmentation fault and core dump.

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

Patch 208.00 OSF350-208	**Patch:** Token Ring Driver Corrections **State:** Supersedes patch OSF350-107 (107.00) This patch corrects the following: • After installation and configuration of a DW300 token ring option, the system becomes unstable on boot, resulting in varied system panics. • The token ring driver, when storing the product_id, can cause corruption which can result in a kernel read access panic.
Patch 211.00 OSF350-211	**Patch:** Kernel Mem Fault Panic (route.o) **State:** Supersedes patch OSF350-197 (197.00) This patch corrects the following: • Fixes a problem in which the system panics when the routing code failed to range check the destination address length. • Fixes a problem which causes kernel memory fault in ubc_sync_iodone() due to corruption of buffer header (struct buf).
Patch 213.01 OSF350-213-1	**Patch:** LSM Volumes Remain In SYNC State **State:** Supersedes patch OSF350-213 (213.00) This patch corrects the following: • Fixes a problem on ASE systems where LSM volumes remain in SYNC state when no volume resync or volplex att command is running. This results in performance degradation.
Patch 216.00 OSF350-216	**Patch:** volrecover -b Command Correction **State:** Existing 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 218.00 OSF350-218	**Patch:** Memory Leak Due To automount Command **State:** Existing Automount can take up more memory than is necessary due to a memory leak.
Patch 221.00 OSF350-221	**Patch:** MFA Driver ESP Self-test Halt/Restart **State:** Existing Fixes a halt/restart problem with the mfa driver ESP self-test.
Patch 223.00 OSF350-223	**Patch:** Security (SSRT0396U) **State:** Supersedes patch OSF350-175 (175.00) This patch corrects the following: • Fixes problems with the rpc.pcnfsd program that can cause rpc.pcnfsd to crash. When rpc.pcnfsd crashes, the pc nfs service will disappear. • A potential security vulnerability has been discovered, where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability.
Patch 224.00 OSF350-224	**Patch:** Support For New European Timezones **State:** Existing Fix European timezones for new EC (European Community) rules for daylight savings time.

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

Patch 231.00 OSF350-231	**Patch:** Incorrect Results From System V getdirentries **State:** Existing Fixes a problem where the System V getdirentries() system call did not correctly calculate the number of entries in a directory inode when accessing the /dev/fd filesystem.
Patch 237.00 OSF350-237	**Patch:** find Command Correction **State:** Existing Fixes a problem in which the find command will not handle more than 100 arguments.
Patch 238.00 OSF350-238	**Patch:** Mail Sent Using uucp Or Output Using uux Error **State:** Existing Mail sent using uucp, or output to Mail from the uux command causes the mail message to be sent from the daemon to root with the following error message: "remote access to path/file denied". The error message is sent to root in a mail message.
Patch 239.00 OSF350-239	**Patch:** ksh Corrections **State:** Supersedes patches OSF350-162 (162.00), OSF350-171 (171.00) This patch corrects the following: • Fixes a problem where an attribute had been set to "read only" and the built-in command typeset (e.g., typeset +r)could not set it back (unset) to "read/write" status. • Fixes 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. • In some cases, the tty modes have been reset. This problem occurs after exiting a ksh session.
Patch 240.00 OSF350-240	**Patch:** showmount -e Command Correction **State:** Existing Add the time out options -t nnn & -T to the "showmount" command.
Patch 241.00 OSF350-241	**Patch:** Incorrect Profiling Data **State:** Existing This patch corrects the following: • Fixes a problem that occurs on a multiprocessor system in which the pfm driver does not provide any profiling data on CPUs other than #0. • Fixes a problem that occurs on systems with recent CPU hardware (EV5) in which using the kprofile command will cause the system to hang.
Patch 247.00 OSF350-247	**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.
Patch 249.01 OSF350-249-1	**Patch:** LMF License Unit Correction For Optical Filesystem **State:** Supersedes patch OSF350-249 (249.00) This patch corrects the following: • Multiple mounts of the same file system under the Optical file system may fail with ERRNO = 169.

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

Patch 250.00 OSF350-250	**Patch:** NFS Memory Handling & NFS mounted PATHWORKS dirs **State:** Supersedes patches OSF350-072 (72.00), OSF350-095 (95.00), OSF350-215 (215.00) This patch corrects the following: • If a file from a remote nfs mounted directory is mmapped, removed on the server, and msynced from the client, the client machine can hang. • Large memory growth of ucred structures can occur. This is especially prevalent if a user is using setuid programs. • Fixes 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.
Patch 252.00 OSF350-252	**Patch:** Unlinking STREAMS Multiplexors Correction **State:** Supersedes patches OSF350-204 (204.00), OSF350-229 (229.00) This patch corrects the following: • SVR4 STREAMS documentation is being violated because a valid device id is not being passed by the push function when a module is pushed on the stream. Instead, a zero value is being set. • A customer-written device driver attempts to return a customer-defined error value that is out of the defined range (0-128) the value EINVAL is returned instead. • Set the device number to zero or the actual value to prevent the hang caused by patch OSF350-229.
Patch 256.00 OSF350-256	**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 263.00 OSF350-263	**Patch:** Mail "From" Incorrect On Incoming Remote Mail Msgs **State:** Existing The first "From" line in an incoming non-local mail message indicates the mail is from "daemon" rather than the actual sender.
Patch 268.00 OSF350-268	**Patch:** mkpasswd Command Correction **State:** Existing Fixes a problem with the mkpasswd command.
Patch 269.00 OSF350-269	**Patch:** Process Hang On SMP System **State:** Existing A process may hang while attempting to obtain a file lock using flock() when run on an SMP system.
Patch 271.00 OSF350-271	**Patch:** SMP System Panic Due To Duplicate namecache Entries **State:** Existing A flaw exists in DIGITAL UNIX SMP systems that results in duplicate namecache entries being created. Under heavy file system lookup operations this can eventually result in a simple lock timeout and a system panic.

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

Patch 273.00 OSF350-273	**Patch:** rmt Command Corrections **State:** Existing Fixes a problem that occurs when using the rmt program to access devices or files.
Patch 274.00 OSF350-274	**Patch:** Quota Support For Numeric User Names And Groups **State:** Existing 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 275.01 OSF350-275-1	**Patch:** Security, rlogin **State:** Supersedes patch OSF350-275 (275.00) This patch corrects the following: • A potential security vulnerability has been discovered, where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability.
Patch 278.00 OSF350-278	**Patch:** dump & rdump Command Correction **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 282.00 OSF350-282	**Patch:** SCSI PMAZC Driver Corrections **State:** Existing This patch corrects the following: • The system can hang after the appearance of binary.errlog entries: sim_err_sm Target went to command phase sim94_intr Illegal command • Fixes a bug in the SIM94 interrupt handler where the target mode flag for a controller was being set before a previous non-target mode request was completed.
Patch 285.00 OSF350-285	**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 286.00 OSF350-286	**Patch:** System Hang Correction **State:** Existing Fixes a problem in which a non-timeshared (i.e., fixed priority) thread running on a multiprocessor system is inappropriately given a priority boost when returning from a funnelled subsystem.
Patch 287.00 OSF350-287	**Patch:** Floating Point Errs On Programs Compiled w/ IEEE mode **State:** Existing Some valid programs compiled with ieee mode may receive a floating-point exception even though they should run to completion.
Patch 289.00 OSF350-289	**Patch:** Compiler Correction **State:** Existing The code generator used an incorrect codegen sequence when doing stack allocation within procedure prologs where the size of the stack was very large (for example, when a structure is passed as an entity rather than as a pointer).

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

Patch 291.00 OSF350-291	**Patch:** cron Command Correction **State:** Supersedes patch OSF350-233 (233.00) 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. • Fixes 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 293.00 OSF350-293	**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 312.00 OSF350X-002	**Patch:** Security, dxconsole, xconsole (SSRT0358X) **State:** Existing A potential security vulnerability has been discovered, where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability.
Patch 313.00 OSF350X-003	**Patch:** Security, dxchpwd (SSRT0356U) **State:** Existing A potential security vulnerability has been discovered, where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability.
Patch 316.00 OSF350X-006	**Patch:** Xfont Server Corrections **State:** Existing The X font server will sometimes crash when serving fonts to a system with big-endian byte ordering such as an NCD X terminal.
Patch 321.00 OSF350X-011	**Patch:** Server Display Postscript **State:** Existing There is a problem in the X server Display PostScript code that can cause incorrect colors to be displayed when using a gray ramp with only two cells with a visual of depth greater than 1.
Patch 325.00 OSF350X-015	**Patch:** Security (SSRT0368U) & xdm, Xlib **State:** Supersedes patches OSF350X-005 (315.00), OSF350X-008 (318.00) Corrects the following xdm and Xlib problems: • xdm may get a segmentation fault when forking a child to manage a new display or X terminal. • Xlib function XAddPixel may not work correctly when the format of the image is ZPixmap and the visual is TrueColor. • A potential security vulnerability has been discovered, where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability.

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

Patch 329.00 OSF350X-019	**Patch:** User Never Added (Specific Circumstances) **State:** Existing Fixes the following problem: If the customer adds a new group 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 330.00 OSF350X-020	**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 331.00 OSF350X-021	**Patch:** Security, libXt **State:** Existing A potential security vulnerability has been discovered, where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability.
Patch 333.00 OSF350X-023	**Patch:** dxterm Support To Suppress ANSI Escape Sequences **State:** Existing Adds the new resource printOnlyPrintables to dxterm. When this resource is set to TRUE (the default is FALSE), dxterm will not output any escape sequences when printing. This is needed for some PostScript printer (filters) that can not handle escape sequences.
Patch 334.00 OSF350-348B	**Patch:** named, screend Corrections **State:** Existing A potential security vulnerability has been discovered in bind, where under certain circumstances users may gain unauthorized access. DIGITAL has corrected this potential vulnerability.
Patch 335.00 OSF350X-025	**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 display to another vendors workstation (HP or Sun).
Patch 336.00 OSF350-297	**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 337.00 OSF350-298	**Patch:** Security (SSRT0362U), Seg Fault Correction **State:** Supersedes patches OSF350-093 (93.00), OSF350-267 (267.00) 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. • On systems running enhanced security, the login process may fail with a segmentation fault.
Patch 339.00 OSF350-301	**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 340.00 OSF350-302	**Patch:** PCI psiop Driver Corrections **State:** Supersedes patch OSF350-030 (30.00) This patch corrects the following: • Correct "siopintr: interrupt for non-initialized controller" boot error. • Fixes a problem that occurs with the NCR 53C8XX driver (psiop) in which the device may not appear to be on the SCSI bus.
Patch 342.00 OSF350-304	**Patch:** Security (SSRT0383U) & PC NFS, rpc.statd Corrcts **State:** Supersedes patch OSF350-178 (178.00) This patch corrects the following: • A potential security vulnerability has been discovered, where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability. • Fixes a problem that occurs 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.
Patch 344.00 OSF350-306	**Patch:** Certain Keyboards Stop Functioning Afer Logout **State:** Supersedes patch OSF350-245 (245.00) This patch corrects the following: • 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 345.00 OSF350-343	**Patch:** Panics With Panic String "Simple Lock:" **State:** Supersedes patch OSF350-026 (26.00) This patch corrects the following: • Fixes a problem that could cause the system to panic displaying the following panic string: "Simple_lock: hierarchy_violation." • System panic with "simple_lock: time limit exceeded" message from vrele().
Patch 346.00 OSF350-308	**Patch:** atmarp Command Corrections **State:** Supersedes patches OSF350-187 (187.00), OSF350-226 (226.00) This patch corrects the following: • A problem exists with the atmarp command when you place a duplicate entry in the ARP table. The system panics with a "kernel memory fault". • There will be a panic from atm_arp when large arp caches are encountered. • 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.

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

Patch 350.00 OSF350X-038	**Patch:** Corrects Memory Leak In The Motif Text Widgets **State:** Supersedes patch OSF350X-035 (398.00) 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 351.00 OSF350-313	**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 355.00 OSF350-317	**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.
Patch 356.00 OSF350-318	**Patch:** ftp Command Correction **State:** Supersedes patch OSF350-090 (90.00) This patch corrects the following: • When using automated login for ftp with the help of a .netrc file, the ACCOUNT FIELD information is not passed to the remote host. • 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.

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

Patch 358.00 OSF350-320	**Patch:** PCI Qlogic Driver Correction **State:** Supersedes patches OSF350-002 (2.00), OSF350-075 (75.00), OSF350-261 (261.00) This patch corrects the following: • Stray interrupts which lock up the PCI bus and hang the system. • Reseating disks in BA356 off P2SE would cause the slot to become inaccessible. • All Alpha/PCI systems that support QLogic fail to boot when two or more tapes are installed on a QLogic/SCSI channel. • Panics: – simple lock time limit exceeded – unable to restart Qlogic(LUN queue after abort) – simple_unlock: minimum spl violation • "CAM_ERROR entry too large" messages. • ASE: Qlogic driver returns incorrect status if the sim driver is unable to correctly respond to an Enable_Lun command from the peripheral driver. • CAM errors when the target NVRAM parameters for either tagged queueing or disconnect privilege enable are disabled. • Data transfer size of 16Mb results in no data transferred. • Probe of isp fails intermittently during boot. The following driver corrections require hardware changes to fully resolve the noted problems: • pcierror panic. These driver changes might help mitigate the occurrence of this panic. Complete solution of the problem will involve some changes in the Tlaser platform code. • Bus Device Resets on narrow or wide SCSI devices. Complete solution of these problems requires both this modified driver and new Qlogic firmware (rev 2.10 or greater). • Data corruption occurs on SCSI write transaction in response to a particular sequence of events on the PCI and SCSI bus. This driver change, in combination with rev 2.10 or greater Qlogic firmware, corrects the problem.
Patch 360.00 OSF350-322	**Patch:** telnet Corrections **State:** Supersedes patch OSF350-140 (140.00) This patch corrects the following: • The terminal line characteristics for telnet with a modem were being reset to 7-bits/no-parity from 8-bits/no-parity. • A problem where telnet dumps core if the USER environment variable is the last variable in the environment list.

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

Patch 362.00 OSF350X-032	**Patch:** PCI HW ATI Mach 64 Graphics CX, GX, & CT **State:** Supersedes patches OSF350X-004 (314.00), OSF350X-010 (320.00), OSF350X-012 (322.00), OSF350X-016 (326.00) PCI Hardware ATI Mach 64 Graphics CX, GX, & CT Corrections: • ATI Mach64 graphics family (e.g., GX, CX, and CT) (PB2GA-FA) problems: – Poor performance during PolyFillSolid operations frequently used by applications such as Netscape. – Multi-screen problems when using 2 ATI Mach64 CX graphics cards on an Alphastation 400. – Dashed lines with a line style of LineOnOffDash are too short. – Sometimes the monitor will lose synchronization or become stuck in power-save mode. • S3 Trio64 graphics card problems: – The first character of the user name is ignored during login. – A cursor warped by software is not recognized by the kernel. – A FillSolid operation with a negative starting point is not always clipped correctly. – Screen "noise" occurs when using resolutions other than 1024x768.
Patch 366.00 OSF350-330	**Patch:** Systems w/ Specific TULIP Ethernet Chips **State:** Supersedes patches OSF350-070 (70.00), OSF350-214 (214.00) This is a MANDATORY patch for all machines containing the DECchip 21040-AA and DECchip 21041-AA (TULIP) Ethernet chips. This patch corrects the following: • Under relatively rare and stressful conditions, the DE500-XA Fast Ethernet interface (tu) will stop receiving packets. This causes the interface to appear hung. • Under certain relatively rare and stressful conditions, the DECchip 21040-AA and DECchip 21041-AA (TULIP) Ethernet chips will corrupt a transmit packet and compute/create the CRC per the corrupted data and send the corrupted packet. • Under heavy system/bus loads, the default programming of the DECchip 21140-AA Fast Ethernet device (DE500), results in excessive framing errors. • Under relatively rare and stressful conditions, the DE500-XA Fast Ethernet interface (tu) will stop receiving packets. • Fixes a system panic, on a SMP system and tu interface, with error message: `System Uncorrectable Machine Check 660 (retry set)`

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

Patch 367.00 OSF350-331	**Patch:** Security, sendmail (SSRT0421U) **State:** Supersedes patch OSF350-254 (254.00) This patch corrects the following: • Fixes a problem in which mail cannot be sent to usernames consisting of uppercase and lowercase letters, for example, FooBar. • Fixes a problem in which mail fails when either of the following conditions occurs: – A large distribution list is used. – A distribution list contains more than 1024 characters. • 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.
Patch 370.00 OSF350-334	**Patch:** DE425 On EISA, Device Configuration Problem **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 371.00 OSF350-335	**Patch:** Security & ftp (SSRT0448U) Corrections **State:** Supersedes patches OSF350-160 (160.00), OSF350-300 (338.00) This patch corrects the following: • Fixes a security issue in which a user using anonymous ftp could be logged in to the root directory. • ftpd core dumps when using anonymous ftp with the ls commmand. • A potential security vulnerability has been discovered, where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability.
Patch 372.00 OSF350-336	**Patch:** Threads Corrections **State:** Supersedes patch OSF350-105 (105.00) This patch corrects the following: • Applications linked with DECthreads will behave as if they have no more memory available to them when they are not even close to the operating system limit. • Corrects a problem where multi-threaded applications will experience a hang on SMP systems.

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

Patch 376.00 OSF350-357	**Patch:** Correction For fsck op, prop list corruption **State:** Supersedes patches OSF350-347 (393.00), OSF350-347-1 (393.01) 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 378.00 OSF350-359	**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 380.00 OSF350-362	**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 ("<...>").
Patch 383.00 OSF350X-033	**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 389.00 OSF350-370	**Patch:** pipe function Correction **State:** Supersedes patch OSF350-008 (8.00) This patch corrects the following: • Fixes the pipe function, occurs primarily on SMP systems, that exits prematurely causing data errors. • Processes can hang and/or become defunct when using fnctl() operation on pipes.
Patch 391.00 OSF350-341	**Patch:** CAM Tape Driver Corrections **State:** Supersedes patches OSF350-032 (32.00), OSF350-165 (165.00) This patch corrects the following: • Attempting to write to a TKZ15 tape drive using compression mode resulted in an error which prevents the drive from being written to. • Fixes "simple_lock: time limit exceeded" panics coming from ctape_close() and ctape_strategy() routines. • Fixes "simple_lock: time limit exceeded".
Patch 395.00 OSF350-351	**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.

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

Patch 396.00 OSF350-353	**Patch:** SCSI Data Corruption Corrections **State:** Supersedes patches OSF350-099 (99.00), OSF350-164 (164.00) This patch corrects the following: • Fixes a panic caused by a "simple lock: time limit exceeded". • When running tape tests on a KZTSA SCSI adapter a data corruption problem was found. This data corruption is only seen on large (> 1Meg) odd byte transfers. It can occur on any tape drive connected to the KZTSA SCSI adapter. • Infrequently, under heavy disk I/O loads, user data can be written to the wrong disk, resulting in data corruption. • When a tape drive was powered off, the HSZ40 rebooted, and the system then panicked with "simple_lock: time limit exceeded". When the system was under heavy load, the following group of three errors was logged into the error logger every few minutes: spo_verify_adap_sanity spo_misc_errors spo_bus_reset • The system panicked with a kernel memory fault while trying to remove an spo resource queue entry • The system panicked with: "xpt_callback: callback on freed CCB"
Patch 399.00 OSF350-373	**Patch:** Security, telnetd, inetd (SSRT0367U) **State:** Supersedes patch OSF350-064 (64.00) This patch corrects the following: • Prevents a long delay while trying to log out using telnet. • A potential security vulnerability has been discovered, where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability.
Patch 400.00 OSF350-374	**Patch:** Library Corrections **State:** Supersedes patches OSF350-199 (199.00), OSF350-315 (353.00), OSF350-368 (387.00) 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. • This patch 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. • The problem of t_rcv NOT setting the error flag (t_errno) when no data is retrieved.

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

Patch 401.00 OSF350-375	**Patch:** Misc nfs_client Problems **State:** Supersedes patch OSF350-006 (6.00) This patch corrects the following: • Fixes a problem in which the system crashes when attempting to NFS mount a text file. • cat'ing files located on an NFS volume can cause an infinite copy.
Patch 403.00 OSF350-378	**Patch:** Library Patches **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 404.00 OSF350-345	**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 405.00
OSF350-352
	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 409.00 OSF350-382	**Patch:** Reduce "NFS stale file handle" Messages Correction **State:** Supersedes patches OSF350-020 (20.00), OSF350-119 (119.00), OSF350-220 (220.00), OSF350-314 (352.00) This patch corrects the following: • Fix greatly reduces the number of "NFS stale file handle" messages logged to an NFS server system console. • Allow 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. • System hang or panic with "kernel memory fault" if an NFS server is given corrupted data. • NFS clients, specifically SUN NFS clients, can not write files based on group membership. OSF clients do not have this problem. • Fixes 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.

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

Patch 410.00 OSF350-383	**Patch:** syslogd Cannot Write /dev/console **State:** Supersedes patch OSF350-188 (188.00) 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 411.00 OSF350-384	**Patch:** Various Sckt, Net, pcktfltr, panic Corr **State:** Supersedes patches OSF350-041 (41.00), OSF350-084 (84.00), OSF350-151 (151.00), OSF350-158 (158.00), OSF350-146 (146.00), OSF350-192 (192.00), OSF350-193 (193.00), OSF350-195 (195.00), OSF350-248 (248.00), OSF350-294 (294.00), OSF350-305 (343.00), OSF350-319 (357.00), OSF350-338 (374.00), OSF350-342 (392.00), OSF350-365 (384.00), OSF350-381 (408.00) 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 • System crashes with "Unaligned kernel space access from kernel mode" (Packetfilter unaligned access panic from ipintr). • When writing packets using the packetfilter on FDDI, there are 14 bytes of corruption in the link layer header of the packet, so the packet appears corrupted on the FDDI ring. • 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(). • An SMP machine running a large number of web server daemons, for example, "ns-httpd" or "httpd", may experience an SMP race condition that will cause the system to panic. • 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 the highly informed system admin. • A user on a remote host can cause a DIGITAL UNIX host to hang or panic. • Fixes a problem in which the system panics when an interface is deleted. • Provides a new tcp level socket option called TCP_NODELACK. This socket option allows a user to force an ack (acknowledge) after each received packet

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

Patch 411.00 continued	• 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. • Fixes a kernel memory fault panic that occurs on SMP platforms. The problem occurs when running the Unicenter product from Computer Associates in conjunction with Oracle software. • Fixes a system panic caused by a Windows95 or WindowsNT system sending an illegal length ping (ICMP)packet. • 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. • Fixes ICMP REDIRECTS. When an ICMP REDIRECT is received, the routing table was updated properly, but the IP layer didn't use the new route information. • Fixes a problem where a system attempts to ping a Digital UNIX system connected to a token ring network and the ping uses a message size that requires fragmentation. The Digital UNIX system receiving the ping cannot respond. The token ring driver displays the following error message to the console and resets the token ring adapter: List Error in transmit
Patch 412.00 OSF350-392	**Patch:** Print Subsystem Corrections, lpr, lpq, lprm **State:** Supersedes patches OSF350-172 (172.00), OSF350-183 (183.00) This patch corrects the following: • Fixes a problem where the lpq command causes the program to crash (segmentation fault). • Print jobs cause existing jobs to be deleted from the queue whenever the number of print queue entries exceeded 1000. • Print jobs created within a short timeframe, for example within the same second, were not sorted by print jobs and timestamps.
Patch 413.00 OSF350-390	**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 415.00 OSF350-348C	**Patch:** uucp Command Corrections **State:** Existing A potential security vulnerability has been discovered in bind, where under certain circumstances users may gain unauthorized access. DIGITAL has corrected this potential vulnerability.

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

Patch 416.00 OSF350-395	**Patch:** vdump & vrestore Command Corrections **State:** Supersedes patches OSF350-159 (159.00), OSF350-205 (205.00), OSF350-389 (201.01), OSF350-391 (414.00) 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 contenets; terminating`

Patch 417.00
OSF350-462
	Patch: Various Kernel Corrections
	State: Supersedes patches OSF350-055 (55.00), OSF350-103 (103.00), OSF350-106 (106.00), OSF350-110 (110.00), OSF350-113 (113.00), OSF350-125 (125.00), OSF350-126 (126.00), OSF350-136 (136.00), OSF350-104 (104.00), OSF350-138 (138.00), OSF350-118 (118.00), OSF350-134 (134.00), OSF350-157 (157.00), OSF350-141 (141.00), OSF350-170 (170.00), OSF350-173 (173.00), OSF350-184 (184.00), OSF350-202 (202.00), OSF350-203 (203.00), OSF350-179 (179.00), OSF350-016 (16.00), OSF350-024 (24.00), OSF350-060 (60.00), OSF350-079 (79.00), OSF350-083 (83.00), OSF350-101 (101.00), OSF350-036 (36.00), OSF350-142 (142.00), OSF350-212 (212.00), OSF350-225 (225.00), OSF350-235 (235.00), OSF350-235-1 (235.01), OSF350-242 (242.00), OSF350-242-1 (242.01), OSF350-264 (264.00), OSF350-265 (265.00), OSF350-014 (14.01), OSF350-098 (98.00), OSF350-166 (166.00), OSF350-227 (227.00), OSF350-258 (258.00), OSF350-251 (251.00), OSF350-082 (82.00), OSF350-135 (135.00), OSF350-277 (277.00), OSF350-280 (280.00), OSF350-284 (284.00), OSF350-290 (290.00), OSF350-295 (295.00), OSF350-321 (359.00), OSF350-360 (379.00), OSF350-360-1 (379.01), OSF350-369 (388.00), OSF350-371 (390.00), OSF350-372 (397.00), OSF350-376 (402.00) OSF350-379 (406.00), OSF350-438 (349.00), OSF350-438-1 (349.01), OSF350-309 (347.00), OSF350-182 (182.00), OSF350-366 (385.00), OSF350-403 (423.00), OSF350-405 (425.00), OSF350-408 (427.00), OSF350-427 (441.00), OSF350-430 (442.00), OSF350-435 (445.00), OSF350-440 (447.00), OSF350-442 (448.00), OSF350-448 (453.00), OSF350-456 (457.00), OSF350-460 (437.00)
	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 a SCSI error recovery problem to allow fast recovery from disk errors.
	• 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`

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

Patch 417.00 continued	• Provides general support for Version A11 KZPSA firmware. • 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 causes systems to panic with a "kernel memory fault" from u_dev_lockop(). This has happened when a database tried to memory map a file. • Fixes an I/O queue corruption problem that occurs during normal shut down of SMP systems with AdvFS. • 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. • Fixes a problem that may occur after a system panics. The system may hang when trying to do a crash dump. • Fixes panics that may occur on SMP systems with message: "simple_lock: time limit exceeded" • Fixes a problem that occurs when running STREAMS. The system panics with a kernel memory fault in either osr_run() or osr_reopen(). • HSZ40s are not logging non-retryable errors in the errorlog. • 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. • When HSZ50 hardware is installed, the system exhibits very slow performance. • 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; they can occur during normal system operations. – Fixes a panic that prints "pmap_dup: level3 PTE not valid". – Fixes a panic that prints "kernel memory fault". • 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.

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

Patch 417.00 continued	• Fixes a number of problems relating to signals and POSIX 1003.1b timers in multithreaded programs running on multiprocessor systems. These problems can result in missed timer-expiration signals and system crashes. • Fixes a problem in which the the lastcomm accounting command doesn't print the "S" flag at appropriate times. This patch also improves the performance of lastcomm. • Fixes system panic with "Zombie walks again" panic message. • The system panics with "ipc_thread_init: reply port allocate" after an unsuccessful port allocation request. • An aio application that calls aio_suspend() with a list of control blocks containing a duplicate address can crash the system if the duplicate aio request has not completed at the time of the call. • A system with large shared memory segments and a large number of users may hang or panic when these users disconnect. The solution here is to make use of unmanaged memory, granularity hints, and shared level 3 page tables. • System Panics: • "thread_depress_wait" on multi-processor machines running multi-threaded applications. • "simple lock owned" panic. • The following kernel memory fault panics: – generated from procfs_readdir()/uiomove(). – fault_pc is in the u_anon_free() routine.in ubc_sync_iodone(). – when a user changes virtual memory (vm) tuning parameters due to slow performance and reboots the machine. – generating a message such as: trap: invalid memory read access from kernel mode – when system is running a number of processes which is > than half the value of npid. – the fault came from malloc or spec_reclaim. – 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. – in simple_lock_B (on multiprocessor system). – in malloc(), in ttyclose(), ttymodem(), and in k_mem_fault

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

Patch 417.00 continued	• "simple_lock_time_violation" panic (problem could also show up as a kernel memory fault panic). • "fill_tlsb: - can not translate address of CPU.\n" panic. • "simple_lock: time limit exceeded" or "cpu_ip_intr: panic request" (on SMP systems running applications that use POSIX realtime timers). • "timeout table overflow" panic when Patch OSF350-060 is installed on multiprocessor system. • Alphaserver 8400 boot panic occurs if the master cpu is not in slot 0. • "simple lock owned" or "simple_lock_fault violation" FAA FDDI driver panics (during restart or re-initialization). • "u_shm_oop_deallocate: reference count mismatch panic. • "pmap_remove_range: page wired" panic. • ‘lock_write: interrupt level call‘ panic. • ‘lock_write: interrupt level call‘ panic. • • Fix memory and process state output from /proc PIOCPSINFO ioctl and SVE ps command. • Cannot kill a multithreaded process. • Processes on a system may block in an uninterruptible state and never run again. This problem occurs when using NFS loopback mounts. • User programs can end with a segmentation violation error when trying to allocate memory that grows in a downward direction. This problem has been seen with Fortran programs that use automatic arrays, and with C programs that use the alloca() function. • A process can hang and a "kill -9" command will not kill it. The ps command will show the status of the process as "U". This is a rare problem that is due to a file system timing problem which occurs during an internal sync and is difficult to reproduce. • When executing with OSF PALcode revision 1.45, or greater, some floating point instructions fail. • When executing with OSF PALcode revision 1.45, or greater, some floating point instructions fail. • Various Alphaserver 8400 errorlog fixes; SMP platform fix to clear MCES register on secondary cpus. • Corrects an SMP/realtime-preemption race condtion in the signal code that can allow a process stopped in sigsuspend to miss a signal wakeup and remaining block indefinitely. • Alphastation 600 5/xxx has reporting/handling problems with single bit ECC Errors.

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

Patch 417.00 continued	• Corrections for Handling Time: – Fix leap-year February time loss problem. – Allow clock to properly wrap at end of year when system is powered down and to prevent clock loosing a day on each reboot during March of a leap year. • Allow clock to properly wrap at end of year when system is powered down and to prevent clock loosing a day on each reboot during March of a leap year. • Corrects 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. • In some adverse situtations the SWXCR controller may hang. • 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. • Processes can become hung during a system call to table(). Debuggers are particularly prone to this problem. • Corrects a problem where a remote user will kill rlogin or telnet and the server host will have an orphanned login process and rlogind or telnetd process in sleep state indefinitely. This is seen only with Asian tty (atty) or any other host which is running c-list rather than STREAMS ttys. • The UNIX kernel crashes during installation if the memory in the system exceeds 1GB. This has only been seen on Lynx-class systems with greater than 1GB of memory.
Patch 418.00 OSF350-397	**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.

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

Patch 420.00 OSF350-400	**Patch:** pax, cpio, tar Command Corrections **State:** Supersedes patches OSF350-047 (47.00), OSF350-303 (341.00), OSF350-333 (369.00) 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. • Fixes pax's tar and cpio archive handling to allow filesizes greater than 4GB. • Disallow pax "b" < 512 to avoid creating corrupt files. • The tar(pax) command doesn't correctly handle sparse files, especially Oracle database files. Pre-allocated space is not replaced on restore.
Patch 424.00 OSF350-404	**Patch:** "simple lock time limit exceeded" System Panic **State:** Supersedes patches OSF350-013 (13.00), OSF350-065 (65.00), OSF350-243 (243.00), OSF350-244 (244.00) This patch corrects the following: • Fixes a problem that occurs on SMP systems using LSM in which the system panics with a "simple lock time limit exceeded" message. • This patch is required for large LSM configurations containing more than 256 plexes or more than 256 volumes. • A system using LSM, AdvFS, and ASE will crash with AdvFS I/O error messages on the console when one volulme of a two-plex LSM mirrored volume is failed out, then recovered, and the other plex is failed out. • In systems where LSM is used with ASE, when there is a SCSI reservation conflict, the LSM configuration daemon, vold, dumps core during an ASE service start and stop. • Fixes several problems that occur during certain LSM operations involving disklabel changes. • Fixes 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`

Patch 426.00
OSF350-407
	Patch: Device Driver Corrections
	State: Supersedes patch OSF350-363 (381.00)
	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.

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

Patch 428.00 OSF350-410	**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".
Patch 429.00 OSF350-411	**Patch:** STREAMS ldtty, Kernel Panic Correction **State:** Supersedes patches OSF350-150 (150.00), OSF350-209 (209.00) 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. • Successive reads wait for VTIME to expire regardless of VMIN setting. • Fixes 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.
Patch 431.00 OSF350-413	**Patch:** audit_tool Command Correction **State:** New patch The audit_tool command hangs if the audit log contains pathnames that encounter boundary conditions.
Patch 433.00 OSF350-418	**Patch:** awk/nawk Command Corrections **State:** Supersedes patch OSF350-056 (56.00) 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 434.00 OSF350-419	**Patch:** FDDI Driver Corrections **State:** Supersedes patches OSF350-145 (145.00), OSF350-367 (386.00) This patch updates the FDDI driver to include: • 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. • 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 up the bumping of some DECnet counters so they could latch to their max values. • Upgrade/Replacement for the "FTA" FDDI driver and fixes a DMA Error which can occur with the older driver.

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

Patch 435.00 OSF350X-037	**Patch:** Bookreader UID Handling, Security (SSRT0349U) **State:** Supersedes patch OSF350X-001 (311.00) This patch corrects the following: • 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. • A potential security vulnerability has been discovered, where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability.
Patch 436.00 OSF350-420	**Patch:** Security, mountd (SSRT0379U,SSRT0496U) **State:** Supersedes patches OSF350-124 (124.00), OSF350-177 (177.00), OSF350-234 (234.00) 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. • 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, 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" can die without logging the event in the daemon.log file and without generating a core file.
Patch 438.00 OSF350-422	**Patch:** Kernel Panic, pty Correction **State:** Supersedes patches OSF350-147 (147.00), OSF350-174 (174.00), OSF350-316 (354.00) This patch corrects the following: • Fixes the problem where applications running System V pseudoterminal slave pty can hang forever on open() system call. • The system becomes totally unresponsive every 2-5 days, not responding to terminals, to the system console, or to pings. • Add support for FIONREAD. • Corrects problem where ntalk daemons are hung. • Fixes a problem that causes the system to "assert_wait" panic with streams code on the stack.
Patch 439.00 OSF350-423	**Patch:** doconfig Hang Correction **State:** New patch Fixes a problem the doconfig program hangs after being invoked by the uuxqt program.
Patch 443.00 OSF350-431	**Patch:** date Command And >1999 Limitation Correction **State:** Supersedes patch OSF350-255 (255.00) 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 444.00 OSF350-432	**Patch:** io_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 446.00 OSF350-437	**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 449.00 OSF350-443	**Patch:** Linker Corrections **State:** Supersedes patches OSF350-086 (86.00), OSF350-120 (120.00), OSF350-168 (168.00), OSF350-246 (246.00), OSF350-276 (276.00), OSF350-337 (373.00) 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. • Numerous previous ld corrections.
Patch 450.00 OSF350-444	**Patch:** ar, nm, odump Command Corrections **State:** Supersedes patches OSF350-049 (49.00), OSF350-262 (262.00) This patch corrects the following: • Fix enables ar to find object modules specified for deletion or extraction whose names are longer than 13 characters. • Failures may occur when nm or odump are run on certain compressed archive libraries built with the ar command. • The ar command -x option, which extracts archive files, may, in error, return a message stating that the file was not found.
Patch 451.00 OSF350-445	**Patch:** Out Of Order Packets, Mem Leak Corrections **State:** Supersedes patch OSF350-288 (288.00) 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.
Patch 452.00 OSF350-446	**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 454.00 OSF350-449	**Patch:** libc Corrections, Security (SSRT0359X) **State:** Supersedes patches OSF350-007 (7.01), OSF350-027 (27.00), OSF350-080 (80.00), OSF350-088 (88.00), OSF350-108 (108.00), OSF350-128 (128.00), OSF350-133 (133.00), OSF350-137 (137.00), OSF350-154 (154.00), OSF350-217 (217.00), OSF350-222 (222.00), OSF350-236 (236.00), OSF350-253 (253.00), OSF350-279 (279.00), OSF350-003 (3.00), OSF350-210 (210.00), OSF350-348 (394.00), OSF350-348-1 (394.01), OSF350-046 (46.00), OSF350-349 (368.00), OSF350-349-1 (348.00), OSF350-398 (419.00), OSF350-412 (430.00) 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 problem where printing of a string with a specified precision could result in a segmentation fault. • /sbin/shutdown takes too long if there are many open LAT lines. • Occasionally, users will still be present in /var/adm/utmp even after they have logged out. • BIND clients cannot perform lookups when given a nameserver address that is an interface alias address on the BIND server. The lookup hangs for a period of time, then times out. 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. • On systems with worldwide support and message catalogs installed: when a locale is set, xdm (the workstation login screen) and the passwd command will core dump when displaying some messages. • sprintf() can add one extra uninitialized character after "%*.*f" format strings if the precision is zero.

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

Patch 454.00 continued	• A dataless system will hang when transitioning from single to multi-user mode. • Multithreaded applications run on V3.2C which use any of the get*_r() functions may dump core or produce incorrect results. • strncat() reads past end of source array. • Fix multiple processes from adding duplicate ut_id lines in the utmp file with duplicate ut-id keys. • Corrects several errors in the syslog entry written by the su program. • 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. • 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(). • The filename pattern-matching behavior of the find command when it includes the "?" metacharacter. The bug actually resides in fnmatch(), which is used by the find command. • In some cases, sendmail generates a core dump when it receives an illegal command, after installing patch OSF350-128. 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. • A heavy load on a NIS server causing more than 32 connections, ypserv would "lose" some of them. Problem is more obvious on ypserv but can occur on ypbind. • NIS slaveservers will not accept a push from the master server of a new map. • A potential security vulnerability has been discovered in BIND (Domain Name Service), where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability. • Fix to allow "getty" to accept uppercase usernames.
Patch 455.00 OSF350-452	**Patch:** "advfsstat -n" Causes A Core Dump **State:** New patch Fixes an AdvFS problem in which the "advfsstat -n" command causes a core dump. The system displays the message: `Memory fault(coredump)`
Patch 456.00 OSF350-454	**Patch:** A Filesystem Cannot Be Unmounted **State:** New patch A filesystem cannot be unmounted and the system displays a "Device busy" error message.

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

Patch 458.00
OSF350-465
	Patch: AdvFS Corrections (AdvFS Consolidated Patch)
	State: Supersedes patches OSF350-037 (37.00), OSF350-038 (38.00), OSF350-058 (58.00), OSF350-094 (94.00), OSF350-123 (123.00), OSF350-127 (127.00), OSF350-148 (148.00), OSF350-163 (163.00), OSF350-181 (181.00), OSF350-219 (219.00), OSF350-259 (259.00), OSF350-272 (272.00), OSF350-232 (232.00), OSF350-283 (283.00), OSF350-292 (292.00), OSF350-324 (363.00), OSF350-328 (365.00), OSF350-356 (375.00), OSF350-380 (407.00), OSF350-424 (440.00)
	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 AdvFS to prevent the following two panics:
	– AdvFS Exception Module = 1, line = 1891
	– kernel memory fault
	• Under heavy I/O loads, systems running with ADVFS and LSM may have sluggish interactive performance, or in DECsafe (ASE) environments, unexpected relocations of services can occur (using AdvFS filesystems).
	• AdvFS will no longer check quotas when user is root.
	• Any access of an AdvFS file could result in the system error messages "write failed, user (group) limit reached" or "quota exceeded too long", even though the file had have not been written to.
	• The vquotaoff command may not report an error if it fails to turn off AdvFS quotas for a fileset.
	• Quotas for AdvFS filesets are not turned off when the filesets are unmounted.

Patch 458.00
continued

- System panics (with AdvFS in use):
  - – The system panics with one of the panic messages:
    - □ "dealloc_bits_page: can not clear a bit twice!"
    - □ "AdvFS Exception Module = 41, Line = 549"
    - □ * "ADVFS EXCEPTION Module = 1, Line = 487, N1 = 0"
    - □ ADVFS EXCEPTION Module = 4, Line = 3541 "bs_unpinpg called with buffer not pinned"
    - □ clear_buf: bufCnt = 0" is too strict and has been removed
    - □ "kernel memory fault" or "ADVFS EXCEPTION panic string: N1= -1027" panics during backup operations using AdvFS
    - □ "simple_lock: time limit exceeded"
    - □ Kernel Memory Fault panics:
      - □ when mounting a crashed AdvFS file system
      - □ Advfs background thread doing I/O to inactive domain
      - □ Advfs background thread doing I/O to inactive domain
  - – When either:
    - □ ls command is run in the fileset mount directory (containing the .tags file)
    - □ msfsck is run at least twice and then the AdvFS fileset is unmounted
- Newly created root filesets may not be assigned the correct unique id while booting the system. Utilities like vdump, find, DECnsr, etc may be unable to distinguish /proc as a mount point due to this problem.
- When AdvFS is the root file system, the system date is incorrect following reboot, even if "date" has been run and the correct date and time entered prior to the reboot.
- After rebooting the system, a file that was changed via mmap() without an msync(), may have corrupted data.
- Large reads can cause Advfs to perform poorly or hang.
- The getrusage system call returns zero for the values of ru_inblock and ru_outblock on an AdvFS file system.
- Fix NFS rpc.lockd "can not clear lock after crash of client" when AdvFS is being used.
- 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".
- An AdvFS system returns an error message when attempting to create greater than 764490 files in a directory.
- System panics with "kernel memory fault" in ubc_page_alloc().
- Idle time is reset on broadcast message when AdvFS is the root file system.
- 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.

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" (OSFPAT00 000400410)

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" (OSFPAT00 001600410)

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" (OSFPA T00000600410)

  Configuring "Patch: Filesystem And vmstat Command Corrections " (OSFPAT000007004 10)

          * 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
```