DIGITAL UNIX

Patch Kit-0006 for Version 4.0
Release Notes and Installation Instructions

June 1998

Product Version: DIGITAL UNIX Version 4.0

This manual describes the contents of Patch Kit-0006, describes how to install and remove patches, and provides other information that you need to know when working with patch kits for the DIGITAL UNIX operating system software.

Digital Equipment Corporation
Maynard, Massachusetts

Contents

About This Manual

This manual contains information specific to Patch Kit-0006 for the DIGITAL UNIX Version 4.0 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-0006.

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-0006.

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 ~42.1 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 ~42.9 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 ~687 KB of storage space is required in /var/adm/patch/doc for patch abstract and README documentation.

  A total of ~71 KB of storage space is needed for the patch management utility.

3.2 Additional Requirements for Systems Running TruCluster Software

If your target system has TruClusters 1.4A (TCR1.4A) installed, do not upgrade the DIGITAL UNIX Operating System patches without the requisite TCR1.4A Patch Kit.

The companion TCR1.4A patch kit for DIGITAL UNIX Patch Kit-0006 is patches.osf-tcr1.4a-[date].tar.z. (The manufacturing date of the kit will be 26Mar1988 or later.)

3.3 Special Instructions for Patch 446.00

3.3.1 Inline Function Performance

Note

Applications using "inline" mutex operations, as described in the pthread.hheader file, will need to RECOMPILE with the application of this patch.The instruction sequences for the pthread_mutex_unlock routine have changed.

Please refer to the existing note in pthread.h entitled “NOTICE: inline function performance vs. binary compatibility" for more information.

3.3.2 mkpasswd Fails To Create ndbm Database

When the /etc/passwdfiles are very large, a performance degradation may occur.

When the number of passwd entries reaches up into the 30,000 to 80,000 range, mkpasswdwill sometimes fail to create an ndbm database. Since the purpose of this database is to allow for efficient (fast) searches for passwd file information, failure to build it causes a serious performance degradation for commands that rely on it.

Using the mkpasswd -scommand to avoid this type of failure could cause a database/binary compatibility problem. If an application that is built statically (non-shared) accesses a password database created by mkpasswd, the application will be unable to correctly read from or write to that database. This would cause the application to fail either by generating ncorrect results, or possibly by dumping core.

Any statically linked application would be affected if it directly or indirectly calls any of the libc ndbmroutines documented in the ndbm(3) reference page and then accesses the password database. To remedy this situation, the application would need to be relinked.

3.4 Special Instructions for Patch 313.00–TZS20 Device Recognition

Warning

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

Note

This assumes the patch is located in /patches.

The installation may be performed at any time, but a reboot is needed for the change to take effect.

Please see the "Patch Kit-0006 Digital UNIX Version V4.0C Installation Instructions".

3.5 Special Instructions for Patch 502.00 - syslogd Correction

The following release note provides information for installing a new version of the syslogdcommand. If your system is configured to forward syslog messages from one host to another, become superuser (for example, root) and manually create a /etc/syslog.authfile.

The /etc/syslog.authfile specifies which remote hosts are allowed to forward syslog messages to the local host. Each remote host name should appear in a separate line in the/etc/syslog.auth file. A line that starts with the '#' character is considered as a comment and is ignored. A host name must be a complete domain name; for example, trout.nyc.com. If a domain host name is

given, it must either appear in the local /etc/hosts file or be able to be resolved by the name server (for example, BIND) that is running on the system.

Note that a host name can have at most as many characters as defined by the MAXHOSTNAMELEN constant in <sys/param.h>. However, each line in the /etc/syslog.authfile can have up to 512 characters.

The /etc/syslog.auth file must be owned by root and have permissions set to 0600.

Unless the domain host name of a remote host is given in the local file, the local host will not log any syslog messages from that remote host.

If the /etc/syslog.authfile does not exist or it exists but is empty or has no valid remote host names in it, the system will assume no remote host is allowed to forward syslog messages to the local host.

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-0006 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 4.0 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-0006 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-0006 and then decided to remove those patches, you would have to specifiy the patch ID of all Patch Kit-0006 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-0006.

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
V4.0D	Full	From V4.0A, V4.0B, V4.0C

6

Summary of Patches

This chapter summarizes all of the patches included in Patch Kit-0006.

Table 6–1 lists patches that have been updated.

Table 6–1: Updated Patches

Patch IDs	Change Summary
Patch 501.00	Superseded by Patch 466.00
Patch 79.00	Superseded by Patch 480.00
Patches 151.00, 171.00, 209.00, 280.00, 505.00	Superseded by Patch 483.00
Patches 54.00, 57.00, 31.00, 48.00, 55.00, 62.00, 32.00, 52.00, 19.00, 19.01, 50.00, 82.00, 99.00, 94.00, 98.00, 100.00, 110.00, 113.00, 114.00, 121.00, 123.00, 127.00, 129.00, 141.00, 165.00, 161.00, 163.00, 194.00, 199.00, 210.00, 212.00, 214.00, 229.00, 221.00, 56.00, 211.00, 228.00, 232.00, 238.00, 239.00, 241.00, 251.00, 264.00, 266.00, 213.00, 21.00, 12.00, 96.00, 108.00, 145.00, 195.00, 196.00, 200.00, 252.00, 255.00, 267.00, 10.00, 268.00, 57.00, 265.00, 278.00, 130.00, 281.00, 286.00, 260.00, 298.00, 300.00, 303.00, 305.00, 310.00, 222.00, 288.00, 292.00, 361.00, 319.00, 326.00, 341.00, 346.00, 358.00, 359.00, 360.00, 365.00, 367.00, 381.00, 391.00, 368.0, 49.00, 104.00, 147.00, 248.00, 366.00, 390.00, 388.00, 384.00, 387.00, 401.00, 395.00, 398.00, 504.00, 481.00, 416.00, 420.00, 421.00, 422.00, 432.00, 441.00, 442.00, 445.00, 449.00, 450.00, 454.00, 456.00, 457.00, 459.00, 464.00, 467.00	Superseded by Patch 468.00
Patches 274.00, 329.00, 383.00, 484.00, 485.00	Superseded by Patch 455.00
Patch 144.00	Superseded by Patch 488.00
Patches 1.00, 45.00, 68.00, 111.00, 105.00. 148.00, 125.00, 191.00, 191.01, 234.00, 247.00, 294.00, 250.00, 275.00, 122.00. 309.00, 270.00, 325.00, 331.00, 356.00, 486.00, 415.00, 437.00, 444.00, 447.00, 471.00, 472.00, 506.00, 478.00, 503.00	Superseded by Patch 503.01
Patches 18.00, 40.00, 59.00, 72.00, 78.00, 84.00, 102.00, 138.00, 237.00, 269.00, 307.00, 269.00, 307.00, 299.00,, 413.00, 426.00, 433.00	Superseded by Patch 462.00
Patch 120.00	Superseded by Patch 414.00
Patch 314.00	Superseded by Patch 502.00
Patches 7.00, 17.00, 22.00, 24.00, 25.00, 27.00, 37.00, 47.00, 39.00, 70.00, 76.00, 80.00, 83.00, 88.00, 93.00, 101.00, 106.00, 119.00, 131.00, 133.00, 139.00, 143.00, 153.00, 154.00, 203.00, 208.00, 223.00, 243.00, 64.00, 246.00, 259.00, 261.00, 277.00, 295.00, 302.00, 312.00, 315.00,, 339.00, 339.01, 332.00, 340.00, 345.00, 354.00, 363.00, 377.00, 389.00, 392.00, 393.00, 397.00, 400.00, 396.00, 407.00, 482.00, 431.00	Superseded by Patch 446.00
Patches 203.00, 296.00, 223.00, 296.01, 323.00	Superseded by Patch 423.00
Patch 136.00	Superseded by Patch 424.00

Table 6–1: Updated Patches (cont.)

Patch 167.00	Superseded by Patch 429.00
Patch 23.00	Superseded by Patch 430.00
Patches 30.00, 35.00, 53.00, 41.00, 67.00, 85.00, 92.00, 142.00, 146.00, 256.00, 333.00, 369.00	Superseded by Patch 434.00
Patch 206.00	Superseded by Patch 435.00
Patches 2.00, 2.01, 2.02, 118.00, 169.00, 157.00, 253.00, 285.00, 316.00, 335.00	Superseded by Patch 436.00
Patches 242.00, 399.00	Superseded by Patch 465.00
Patches 91.00, 149.00, 201.00, 273.00	Superseded by Patch 470.00
Patch 107.00	Superseded by Patch 474.00
Patches 173.00, 321.00	Superseded by Patch 475.00
Patches 177.00, 178.00, 492.00	Superseded by Patch 494.00
Patch 225.00	Superseded by Patch 493.00
Patches 183.00, 244.00, 289.00	Superseded by Patch 496.00
Patches 216.00, 272.00, 322.00	Superseded by Patch 495.00
Patches 186.00, 189.00, 320.00, 403.00, 498.00	Superseded by Patch 499.00

Table 6–2 provides a summary of patches in Patch Kit-0006.

Table 6–2: Summary of patches in Patch Kit-0006

Patch IDs	Abstract
Patch 11.00 OSF400-011	**Patch:** C Programs Generated By lex **State:** Existing Programs generated by lex that use the %pointer definition in the lex grammar file produce a memory fault and a core dump.
Patch 29.00 OSF400-029	**Patch:** Data Corruption (Symbios 810A/825A/860/875 chips) **State:** Existing Data corruption due to change in DNAD register behavior on Symbios 810A/825A/860/875 chips.
Patch 33.00 OSF400-033	**Patch:** "ping -p ff" Results In Segmentation Fault/Core Dump **State:** Existing This patch corrects the problem where "ping -p ff" results in a segmentation fault and core dump.
Patch 36.00 OSF400-036	**Patch:** showmount Command Correction **State:** Existing Add the time out options -t nnn & -T to the 'showmount' command.
Patch 42.00 OSF400-042	**Patch:** NIS Slaveserver Correction **State:** Existing NIS slaveservers will not accept a push from the master server of a new map.
Patch 58.00 OSF400-058	**Patch:** gated Daemon Corrections **State:** Existing This patch allows a system that is running gated to update internal routing tables to manage the router discovery function.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 61.00 OSF400-061	**Patch:** at Command Correction **State:** Existing This patch fixes a problem that occurs on multiprocessor machines in which the 'at' command causes extra batch jobs to be executed. Sometimes temporary files are created and not removed, causing the queue limit to be exceeded.
Patch 69.02 OSF400-069-2	**Patch:** Rsh and sh Command Corrections **State:** Supersedes patches OSF400-069 (69.00), OSF400-069-1 (69.01) This patch corrects the following: • Corrects the following problems that occur when an application is started from a subshell, for example, sh -c <command>: • An application will hang if it receives an interrupt signal, for example, if the user enters Ctrl/C. • While an application is running, if Ctrl/C is entered, the parent process exits, but the child process remains.
Patch 74.00 OSF400-074	**Patch:** Security, rlogin (SSRT0416U) **State:** Existing A potential security vulnerability has been discovered in "rlogin", where under certain circumstances users may gain unauthorized access. DIGITAL has corrected this potential vulnerability.
Patch 81.00 OSF400-081	**Patch:** ZLXp-L1 or ZLXp-L2 Graphics Option Corrections **State:** Existing This patch corrects the following ZLXp-L1 or ZLXp-L2 graphics option problems: • Stereo mode (XStereo) does not function properly. • Applications that use the second hardware colormap do not display the correct colors.
Patch 89.00 OSF400-089	**Patch:** Security, ris_pax (SSRT0413U) **State:** Existing A potential security vulnerability has been discovered in 'ris_pax', where under certain circumstances users may gain unauthorized access. DIGITAL has corrected this potential vulnerability.
Patch 90.00 OSF400-090	**Patch:** PowerStorm 4D20 Graphics Option Monitor Resolution **State:** Existing On system with a PowerStorm 4D20 (TGA2) graphics option, monitor resolution setting 4 (1600x1200 at 65 Hz) is not setup properly.
Patch 95.00 OSF400-095	**Patch:** FDDI DEMFA Driver Corrections **State:** Supersedes patch OSF400-044 (44.00) This patch corrects the following: • A halt/restart problem with the FDDI DEMFA driver when the interface performs the ESP self tests.
Patch 117.00 OSF400-117	**Patch:** Ping Command Timeout Correction **State:** Existing Ping command can time out after invoking the "rcinet restart" command.
Patch 126.00 OSF400-126	**Patch:** Kernel Memory Fault in dqget() Routine Correction **State:** Existing This patch fixes a "kernel memory fault" in the dqget() routine.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 128.00 OSF400-128	**Patch:** Corrections For Various Keyboards **State:** Supersedes patch OSF400-124 (124.00) This patch corrects the following: • On systems with PCXAL, LK411, and similar keyboards, sometimes on boot or between sessions on the workstation monitor, the keyboard stops working. • Issuing a SET_DEVICE_MODE ioctl to the workstation driver to change cursor reporting to relative mode fails.
Patch 140.00 OSF400-140	**Patch:** ATI Mach64 Graphics Card Monitor Handling **State:** Existing On systems with an ATI Mach64 graphics card, sometimes the monitor goes into power-save mode and cannot be restored.
Patch 150.00 OSF400-150	**Patch:** Incorrect Terminal Line Characteristics **State:** Supersedes patch OSF400-075 (75.00) This patch corrects the following: • Prevents terminal line characteristics for telnet with a modem to be reset to 7-bits/no-parity from 8-bits/no-parity. Incorrect terminal line characteristics cause garbage to be displayed when using telnet. • Fixes a problem where telnet dumps core if the USER environment variable is the last variable in the environment list.
Patch 152.00 OSF400-152	**Patch:** /sbin/loader Corrections **State:** Existing This patch fixes a problem that may cause /sbin/loader to fail to resolve duplicate symbols in dlopen'ed shared libraries.
Patch 160.01 OSF400-160-1	**Patch:** Mail Corrections, Security (SSRT0421U) **State:** Supersedes patches OSF400-063 (63.00), OSF400-071 (71.00), OSF400-071-1 (71.01), OSF400-160 (160.00) This patch corrects the following: • If the user sending mail makes an error entering the destination address the user will receive a mail message that contains both the text of the mail and the error messages. The error messages do not correctly describe the exact nature of the problem. • Fixes a problem that can occur with programs linked with libaio. These programs could dump core with a SIGSEGV signal or corrupt memory when calling the close() function with a bad file descriptor value. • 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 164.00 OSF400-164	**Patch:** OSF400-164 **State:** Existing This patch fixes a problem that can occur with programs linked with libaio. These programs could dump core with a SIGSEGV signal or corrupt memory when calling the close() function with a bad file descriptor value.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 166.00 OSF400-166	**Patch:** Full Duplex Mode Setting on DEFPA Correction **State:** Existing This patch fixes a problem in which settting full duplex mode on DEFPA using "/usr/sbin/fddi_config -i fta0 -x1" will not enable full duplex mode.
Patch 168.00 OSF400-168	**Patch:** netstat Command Output Correction **State:** Existing This patch fixes a problem in which "netstat -I fta0 -s" reports 6 bytes of the 8 byte "Station UID" and "Station ID".
Patch 170.00 OSF400-170	**Patch:** Dynamically Configured Device Drivers On An EISA Bus **State:** Supersedes patch OSF400-020 (20.00) This patch corrects the following: • Fixes a problem in which dynamically configured device drivers on an EISA bus may fail to configure into the kernel. Apply this patch if your system supports a loadable EISA bus driver. • Fixes two problems that occur on systems with an EISA bus: – A system running four DE425 adapters off an EISA bus may hang. – If a device's EISA configuration file contains a function DISABLE keyword and the DISABLE option is selected, the device's driver may not be configured and probed at bus configuration time.
Patch 172.00 OSF400-172	**Patch:** mailx Command Correction **State:** Existing This patch fixes two problems with the mailx command.
Patch 175.01 OSF400CDE-001-1	**Patch:** CDE Session Manager Inhibits Unaligned Access Msgs **State:** Supersedes patch OSF400CDE-001 (175.00) This patch corrects the following: • Corrects a problem where applications behave as if 'unaligned access' error messages have been suppressed. This can lead to poor application performance without a visible cause.
Patch 179.00 OSF400CDE-005	**Patch:** Window Manager Correction **State:** Existing This patch fixes two problems with the CDE window manager. In the first problem, the CADDS5 (a third party cad tool) text window tends to walk off the screen. In the second problem, the CDE icon box moves 29 pixels higher along the x axis each time the user's home session is resumed.
Patch 180.00 OSF400DX-001	**Patch:** dxsysinfo Corrections **State:** Existing This patch corrects the following: • dxsysinfo causes the X server's colormap entries to be corrupted. • dxsysinfo may display certain filesystem percent full values incorrectly. • dxsysinfo repeatedly adds device /dev/prf as a tape entry into its Device Information Area. • dxsysinfo leaves its child process orphaned after a logout. • Hard disk icons fail to display in the Device Information Area when the colormap is full or on a black/white screen.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 181.00 OSF400DX-002	**Patch:** OSF400DX-002 **State:** Existing This patch adds the new resource printOnlyPrintables to dxterm. When this resource is set to TRUE (the default is FALSE), dxterm will not output any escape sequences when printing. This is needed for some PostScript printer (filters) that can not handle escape sequences.
Patch 185.00 OSF400X11-002	**Patch:** X Server Performance Is Slow (Drawing Arcs) **State:** Existing Server performance is slow when an application is drawing arcs which are outside the bounds of the drawable window.
Patch 188.00 OSF400X11-009	**Patch:** ATI Mach64 Graphics Card Monitor Handling **State:** Supersedes patch OSF400X11-001 (184.00) This patch corrects the following: • On an AlphaStation 400 with two ATI Mach64 CX graphics cards (dual-screen), the display on the second screen is corrupted at 1280x1024 resolution. • On systems with an ATI Mach64 graphics card, sometimes the monitor will lose synchronization or become stuck in power-save mode.
Patch 192.00 OSF400-177	**Patch:** LEX Correction **State:** Existing This patch fixes a LEX problem. Without this patch, LEX rejects quoted regular expressions where the ending quote is preceded by a double backslash, as in: "\\"xxx, and produces the following message: "lex:(Warning at line 8)Non- terminated string"
Patch 193.00 OSF400-179	**Patch:** CD/DSR Not Dropping Right Away After Dial-out **State:** Existing uugetty - CD/DSR not dropping right away after dial-out.
Patch 197.00 OSF400-183	**Patch:** rwhod Correction **State:** Existing rwhod Correction This patch fixes a problem in which rwhod daemon can cause a core dump with a segmentation fault.
Patch 198.00 OSF400CDE-006	**Patch:** : Nodename Length Correction **State:** Existing This patch fixes a problem in which users logging into a system that has a nodename longer than 32 characters cause ttsession to core dump. This only happens when using CDE desktop.
Patch 204.00 OSF400-190	**Patch:** automount Utility Correction **State:** Existing Automount program has a memory leak. In some cases, this leak can cause applications to hang. The daemon.log file shows the following error message: Memory allocation failed: not enough space
Patch 205.00 OSF400-191	**Patch:** NTP Correction **State:** Existing This patch fixes a problem where the NTP deamon (xntpd) does not work using a Spectracom radio clock as a reference.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 207.00 OSF400-194	**Patch:** cron Command Correction **State:** Existing This patch 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 215.00 OSF400-203	**Patch:** auth_for_terminal() Segmentation Fault Correction **State:** Supersedes patch OSF400-115 (115.00) This patch corrects the following: • Under enhanced security, sometimes users (even root) are unable to log in on graphics console, even after using dxdevices or edauth to clear the t_failures count. • On systems running enhanced security, user-written applications that call auth_for_terminal() may fail with a segmentation fault.
Patch 218.00 OSF400-205	**Patch:** dbx Correction **State:** Existing This patch fixes a problem that causes dbx to hang when stepping past a system() function call.
Patch 219.00 OSF400-206	**Patch:** OSF400-206 **State:** Existing This patch fixes a problem in which the tic command incorrectly returns a non-zero exit value upon successful completion. An exit value of 0 should be returned upon successful completion.
Patch 224.00 OSF400CDE-007	**Patch:** Security, (SSRT0438U) **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 potential vulnerability.
Patch 227.01 OSF400-211-1	**Patch:** dd Command Correction **State:** Supersedes patch OSF400-211 (227.00) This patch corrects the following: • Fixes a problem in which the dd command can corrupt output on very large files (2GB or greater) when the "conv=sparse" option is used.
Patch 233.00 OSF400X11-014	**Patch:** Screen Flickers in Power-save Mode Correction **State:** Supersedes patch OSF400X11-013 (226.00) This patch corrects the following: • On systems with PowerStorm 4D40T, 4D50T, or 4D60T graphics options, the X server may hang every 49 days. • Screen flickers on and off when in power-save mode.
Patch 236.00 OSF400DX-007	**Patch:** DECwindows Session Manager Correction **State:** Existing This patch fixes the following problems in the DECwindows Session Manager (dxsession) application. Ungraceful exit can be made through the window manager's 'Close' button, whose behavior is inconsistent with that of dxsession's 'End Session' button.
Patch 240.00 OSF400-223	**Patch:** talkd Correction, Security (SSRT0446U) **State:** Existing A potential security vulnerability in talkd has been corrected.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 245.00 OSF400CDE-009	**Patch:** dtksh Command Correction, (SSRT0435U) **State:** Existing This patch corrects two problems that occur when using the dtksh command: • dtksh can lose output lines when a pipe or I/O indirection is used. • The following error message may be displayed after using a pipe in dtksh: dtksh: hist_flush: EOF seek failed errno=9
Patch 249.00 OSF400-230	**Patch:** acctcom Command Correction **State:** Existing This patch fixes a problem in which the size field of a process displayed by the acctcom command is displayed incorrectly.
Patch 262.00 OSF400-243	**Patch:** kloadsrv May Cause System Panic **State:** Existing This patch fixes a problem in which loadable kernel modules that are loaded with the kloadsrv daemon at run time, may cause a system panic.
Patch 263.00 OSF400-246	**Patch:** rpc.lockd Correction **State:** Existing This patch fixes several problems with the network lock daemon, rpc.lockd: • NFS mounted file systems may hang. • An error occurs with NFS mounted user mail files. This error prevents the files from being locked and prints out the following message: cannot lockf • An NFS problem may occur. The system displays the following error message: NFS error 48 cannot bind sockets
Patch 271.00 OSF400-255	**Patch:** Simple Lock Time Limit Exceeded Panic **State:** Existing This patch fixes a problem that occurs on SMP systems using LSM in which the system panics with a "simple lock time limit exceeded" message.
Patch 279.00 OSF400-263	**Patch:** ar Command Correction **State:** Supersedes patch OSF400-046 (46.00) This patch corrects the following: • The ar command's -x option, which extracts objects from archive files, may incorrectly output a message stating that the file was not found. • Fixes the following problems with the ar command: – When creating or modifying an archive, the ar command may leave a large file in /tmp or in the current directory (when the -l option is used). – If Patch 46.00 was previously installed (OSF400-046), the ar command cannot find object modules specified for deletion or extraction if the file name is longer than 13 characters. An error message similar to the following is displayed: ar: Error: button_previous.gif not found

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 283.00 OSF400-268	**Patch:** Problem, System Time Using MICRO_TIME Kernel Config **State:** Existing This patch fixes several problems with system time when the MICRO_TIME kernel configuration option is used. It resolves a one second delay in updating secondary processors after changing the system time. BOOTTIME is now written properly to utmp from a secondary processor during boot. Processors are immediately updated when brought on-line during boot or via the psradm utility.
Patch 284.00 OSF400-269	**Patch:** yppasswd Command Correction **State:** Existing This patch fixes a problem in which yppasswd users get the error "password mismatch, password unchanged" creating passwords longer than 8 characters.
Patch 287.00 OSF400CDE-010	**Patch:** CDE Application Builder Core Dump Correction **State:** Supersedes patch OSF400CDE-002 (176.00) This patch corrects the following: • The CDE Application Builder will core dump on second attempt to add pulldown menus to a menubar item. • The application builder (dtbuilder) core dumps when changing the default button in the revolving property editor.
Patch 291.00 OSF400-280	**Patch:** faa FDDI Driver Kernel Memory Fault Correction **State:** Existing This patch fixes a kernel memory fault caused by the faa FDDI driver. The panic was due to incomplete handling of an error condition by the driver ("Timeout in command request"). The command request buffer was freed, however the reference to it was not removed from the command request list. When this list. When this list was later accessed, the invalid memory reference panic occurred.
Patch 293.00 OSF400-282	**Patch:** quotas For Filesystems Causes rpc.rquotad To Hang **State:** Supersedes patch OSF400-214 (230.00) This patch corrects the following: • Fixes a problem in which the rpc.rquotad daemon hangs when using quotas for NFS filesystems in a TruCluster or Available Server (ASE) v1.4 environment. • Fixes the following problems with the rpc.rquotad: – When the NFS server is a member of an ASE or TruCluster environment, the rpc.rquotad daemon may exit abnormally. The abnormal exit causes the quota command on NFS clients to not report quotas for NFS mounted file systems. – When the quota command is repeatedly run from a remote system, the virtual size of the rpc.rquotad daemon on the local system will grow due to a memory leak.
Patch 297.01 OSF400-189C-1	**Patch:** uucp Command Correction (SSRT0296U) **State:** quotas For Filesystems Causes rpc.rquotad To Hang This patch corrects the following: • A potential security vulnerability has been discovered in BIND (Domain Name Service), where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 301.00 OSF400-290	**Patch:** lpq Command Correction **State:** Existing This patch fixes a problem where the lpq command causes the program to crash (Memory fault).
Patch 304.00 OSF400-295	**Patch:** HX (PMAGB-BA) Graphic Mouse Cursor Correction **State:** Existing This patch fixes a problem with the mouse cursor when the system contains the HX (PMAGB-BA) graphics option. The cursor offset is incorrect on the Y Axis by 2 pixels.
Patch 306.01 OSF400-299-1	**Patch:** comm Command Correction **State:** Supersedes patch OSF400-299 (306.00) This patch corrects the following: • Fixes a problem with the comm command. The comm command may split input lines that are greater than 255 characters in length by inserting a <carriage return> in the line when written to an output file. In some cases, characters will be truncated.
Patch 313.00 OSF400-303	**Patch:** ddr_config Corrections **State:** Supersedes patches OSF400-066 (66.00), OSF400-218 (235.00), OSF400-218-1 (235.01) This patch corrects the following problems with ddr_config: • DDR subsystem updated to handle SCSI devices returning a non-standard device type. • ddr_config would sometimes build partial device records. • ddr_config on DIGITAL UNIX V4.0 was not compatible with input files created prior to this version. • Adding support for TZS20, and device recognition for TZS2, TLZ10, and TLZ1 tape drives.
Patch 317.00 OSF400-305	**Patch:** diff Command Correction **State:** Existing This patch fixes a problem related to misinterpretation of multibyte characters by the diff command. The problem also affects the delta command of SCCS. The symptom of the problem in the diff command is that it sometimes treats a text file containing multibyte characters as a binary file. The symptom of the problem in the delta command is that it sometimes fails to check in a program source file containing multibyte characters.
Patch 318.00 OSF400-309	**Patch:** S3 Trio64V+ Graphics Card Incorrectly Identified **State:** Existing The S3 Trio64V+ graphics card (PB2GA-JC or PB2GA-JD) is not being uniquely identified by the driver at startup.
Patch 328.00 OSF400DX-012	**Patch:** Bookreader Corrections, (SSRT0514U) **State:** Supersedes patch OSF400DX-003 (182.00) This patch corrects the following: • Bookreader aborts with a segmentation fault when displaying certain pages if the required fonts are not available. This problem usually occurs when redirecting Bookreader's display to another vendor's workstation (HP or Sun). • A potential security vulnerability has been discovered, where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 330.00 OSF400-321	**Patch:** Corrects X.25 Crash On AlphaServer 1000 **State:** Existing This patch fixes a problem in which the io_zero() system call returns an incorrect value on an AlphaServer 1000.
Patch 334.00 OSF400-325	**Patch:** atom Command Corrections **State:** Existing This patch fixes the following problems: • The atom command terminates with SIGSEVG signal if the threaded program being instrumented has a stripped shared library. • The "atom -all -env threads" command produces an instrumented version of a threaded (eg DCE) application that will not execute correctly, with either "-tool third" or "-tool hiprof" tool options.
Patch 336.00 OSF400-327	**Patch:** System Crash With >1GB Of Memory **State:** Supersedes patch OSF400-103 (103.00) This patch corrects the following: • AlphaServer 2100A systems crash during boot with greater than 1GB of memory installed. • Fixes a problem that occurs on an AlphaServer 2100A system. When the system is shut down using the "shutdown -r" command, the system will not reboot.
Patch 342.00 OSF400-337	**Patch:** Memory Leak With (dlb) Pseudodevice Driver **State:** Existing This patch fixes a problem that causes the 'doconfig' program to hang when invoked by the uuxqt program.
Patch 343.00 OSF400-339	**Patch:** Security Patch, (SSRT0476U) **State:** Supersedes patches OSF400-086 (86.00), OSF400-267 (282.00) This patch corrects the following: • Allows user control messages to be passed between a STREAMS pty pair. This is a new feature. • Applications running System V pseudoterminal slave pty can hang forever on open() system call. • A potential security vulnerability has been discovered, where under certain circumstances, a kernel memory fault panic may occur.
Patch 344.00 OSF400-340	**Patch:** Enhancements To date Command For Year 2000 Support **State:** Supersedes patch OSF400-043 (43.00) This patch corrects the following: • Enhancements to the date command for Year 2000 support. • Fixes the problem in which 'date' command is unable to set the date to January 1, 1970 00:00:00 GMT or February 29, 2000.
Patch 347.00 OSF400-343	**Patch:** mountd Command Correction, (SSRT0496U) **State:** Supersedes patch OSF400-034 (34.00) This patch corrects the following: • mountd dies without logging the event in the daemon.log file and there is no core file. • 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-0006 (cont.)

Patch 350.00 OSF400-331B	**Patch:** uusend And uustat Command Correction **State:** Supersedes patch OSF400-331 (339.00) This patch corrects the following: • Allows the uusend, uustat, uucpd, and uudecode commands to work correctly when the customer builds a hashed passwd database using a non-default page file block size.
Patch 351.00 OSF400-331C	**Patch:** mkpasswd -s Command Correction **State:** Supersedes patch OSF400-331 (339.00) This patch corrects the following: • Allows customers to create hashed passwd databases from large passwd files by using a new option (-s) to the mkpasswd command. The -s option increases the block size of the database page file.
Patch 352.00 OSF400-331D	**Patch:** OSF400-331D **State:** SUPERSEDED PATCHES: OSF400-331 (339.00) This patch corrects the following: • Allows the uusend voliod commands to work correctly when the customer builds a hashed passwd database using a non-default page file block size.
Patch 353.00 OSF400-122B	**Patch:** quota Command Corrections **State:** Supersedes patches OSF400-073 (73.00), OSF400-112 (112.00), OSF400-122 (122.00) This patch corrects the following: • Correct quota command to return worst error status on exit. • Allows system managers to both set and obtain quotas for users and groups which are numeric when using the edquota, vedquota, quota and vquota programs. • Correct quota command to return most severe error status on exit.
Patch 357.00 OSF400-349	**Patch:** Packet Reception On DE500-XA PCI Fast Ethernet Card **State:** Supersedes patches OSF400-015 (15.00), OSF400-162 (162.00) This patch corrects the following: • Fixes a problem that occurs on an SMP system with a tu (Tulip) Ethernet interface. The system panics with the following error message: System Uncorrectable Machine Check 660 (retry set) • Corrects a problem where packet reception on the DE500-XA PCI Fast Ethernet interface (device mnemonic "tu") comes to a halt under heavy system and network load. • An enhancement to the ethernet driver for the DE500-XA Fast Ethernet Interface. This patch improves the failover time in an ASE environment when the cluster members use DE500-XA interfaces.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 364.00 OSF400-358	**Patch:** awk Utility Correction **State:** Supersedes patch OSF400-318 (327.00) This patch corrects the following: • Fixes problem in which 'awk' consumes memory until the machine swaps itself and core dumps with following error: write failed, file system is full Memory fault - core dumped • Fixes a problem in which the awk -FS command does not display the correct output.
Patch 370.00 OSF400-359	**Patch:** auditmask Utility Correction **State:** Existing This patch fixes a problem that affects systems running the audit subsystem. When reading directives from a file, the auditmask utility does not correctly handle lines formatted as follows: event fail
Patch 371.00 OSF400-371	**Patch:** uprofile And Kprofile Command Corrections **State:** Existing This patch fixes the following problems: • The uprofile and kprofile commands report incorrect statistics on an SMP system or when trying to measure EV5 events other than cycles. • The pfm driver ioctl PCNT5GETCNT returns incorrect data. • An unstoppable stream of pfm interrupts is produced if an EV5 machine is rebooted with the pfm driver active. • The pfm(8), uprofile(1), and kprofile(1) manpages do not describe the EV5 statistics supported by the software. All users of the pfm driver and uprofile or kprofile commands should install this patch.
Patch 372.00 OSF400-370	**Patch:** Correction To volunroot, volrootmir, vol-reconfig **State:** Existing This patch fixes several LSM problems related to the volunroot, volrootmir, and vol-reconfig scripts.
Patch 373.00 OSF400-364	**Patch:** System Run Level Correction **State:** Existing This patch fixes two system run level problems: • On a system running LSM, whenever there is a run level change, the lsmbstartup script runs. This causes root to be mounted read/write in single-user mode. • The bcheckrc command script continues to run even if there is an invalid root entry. This leaves the system in an unusable state in single-user mode.
Patch 375.00 OSF400-365	**Patch:** btree File Format Correction **State:** Existing This patch fixes a probem that affects systems using databases with the btree file format. Only applications using btree in libdb.a or libdb.so are affected and may return incorrect data or crash.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 376.00 OSF400-375	**Patch:** Linker Corrections **State:** Supersedes patches OSF400-038 (38.00), OSF400-077 (77.00), OSF400-174 (174.00) This patch corrects the following: • Changes how the linker handles permission problems with chmod(), corrects an internal linker hang, and removes an unnecessary data segment boundary check for OMAGIC (impure) object files. • A performance problem that the linker has with hidden symbols (-hidden flag) and large numbers of shared library files (.so files). • Fixes a problem where use of "ld -r" will change symbol preemption behavior. • Fixes four linker problems: Hidden/export symbols, Assert getting generated with R_GPVALUE relocations, improper Text segment alignment processing, and linker memory managment problem processing c++ symbols.
Patch 378.00 OSF400-377	**Patch:** Packets Out of Order On PATHWORKS Netbuei Clients **State:** Supersedes patch OSF400-097 (97.00) This patch corrects the following: • Corrects a problem with packets out of order experienced by some PATHWORKS Netbuei clients. • Fixes a memory leak problem that occurs with the STREAMS Data Link Bridge (dlb) pseudodevice driver. This problem could cause a "freeing free mbuff" panic when system memory is exhausted.
Patch 379.00 OSF400CDE-011	**Patch:** dtmail Correction **State:** Existing This patch lets dtmail correctly display Japanese and Korean mail messages that do not have a Content-Type header.
Patch 382.00 OSF400X11-020	**Patch:** Motif Toolkit Correction **State:** Supersedes patches OSF400X11-012 (202.00), OSF400X11-015 (254.00) This patch corrects the following: • Fixes the following problem in the Motif toolkit. The drag-n-drop operation fails, which may cause Motif applications to abort. • Fixes the following problems in the Motif toolkit. Message strings with consecutive newline charaters("\n\n"), lose one newline for every two specified. A character height of zero is possible, and the message box containing the string will not be resized properly. • A potential security vulnerability has been discovered, where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability. • Fixes the memory leak in the Motif text widget when changing colors using XtVaSetValues().
Patch 386.00 OSF400-383	**Patch:** Correction To llogin Command **State:** Existing This patch corrects a problem when exiting an llogin session. If the user does not enter a carriage return to display the shell prompt, the llogin will process continue to run, consuming all the free CPU time available.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 394.00 OSF400-390	**Patch:** ex And vi Editor Corrections **State:** Supersedes patch OSF400-204 (217.00) This patch corrects the following: • Fixes several problems in the ex and vi editors. – Blank lines in the .exrc file prevent the vi editor from executing. – The ex editor does not properly manage the file name buffers when a "write append" command fails. – The vi editor may erroneously report a "Bad file number" error message when switching between files. • The vi editor may erroneously report a "Bad file number" error message when switching between files.
Patch 402.00 OSF400-999	**Patch:** pthread_mutex_destroy() Fails With EBUSY Correction **State:** Supersedes patches OSF400-330 (337.00), OSF400-331-1 (339.01), OSF400-351 222.00), OSF400-250 268.00) OSF400-210 (223.00), OSF400-241 261.00), OSF400-275 (290.00), OSF400-065 (65.00), OSF400-014 (4.00) This patch corrects the following problems: • 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. • When the /etc/passwd file is very large, a performance degradation may occur. • Over time, a multithreaded application may find that asynchronous signals are not being delivered to it.
Patch 404.00 OSF400X11-016	**Patch:** S3 Trio64 Graphics Card Can Lose Time **State:** Supersedes patch OSF400X11-011 (190.00) This patch corrects the following: • Systems with an S3 Trio64 graphics card can loose time (on the order of a few minutes a day). • On systems with an S3 Trio64V+ graphics card (PB2GA-JC or PB2GA-JD), the X server hangs while drawing the login screen.
Patch 405.00 OSF400X11-019	**Patch:** DECwindows Motif toolkit **State:** Existing This patch fixes the following problem in the Bookreader library, which is part of the DECwindows Motif toolkit. When called from an application, bookreader changes the caller's effective UID to the real UID, but then never restores it to the original effective UID, before returning control to the calling program. If an application like dxchpwd is run from a non-root account, it fails with a privilege violation.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 409.00 OSF400-215B	**Patch:** Realtime Library, POSIX Message Queue Functions **State:** Supersedes patches OSF400-109 (109.00), OSF400-109-1 (109.01), OSF400-215 (231.00) This patch corrects the following: • When setting the date with the clock_settime rtl service routine, the date will not get past the date of 'Sat Sep 8 19:46:39 2001' If you try to set past this date the routine returns a EINVAL error. • Fixes a problem in which a system running POSIX message queue functions in the realtime library will either exhibit message queue data corruption or it will hang.
Patch 410.00 OSF400-410C	**Patch:** Math Library Function Corrections **State:** Supersedes patches OSF400-331-1 (39.01), OSF400-241 (261.00), OSF400-210 (223.00), OSF400-154 (154.00) This patch corrects the following: • Fixes the problem of the math library functions not returning the correct NaN value as defined in the Alpha AXP Architecture Reference Manual (Second Edition). • Fixes a problem with fastmath functions F_Exp() and F_Pow() that would cause floating exception core dumps.
Patch 411.00 OSF400-404	**Patch:** Security, (SSRT0487U) **State:** New patch A potential security vulnerability has been discovered, where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability.
Patch 412.00 OSF400-406	**Patch:** Security, (SSRT0495U) **State:** New patch 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 414.00 OSF400-412	**Patch:** Security, (SSRT0456U) **State:** Supersedes patch OSF400-120 (120.00) This patch corrects the following: • Fixes a problem that occurs in ASE/TCR environments in which the rpc.statd daemon does not start when using the -p option to specify a log pathname (> 45 characters). When this happens, NFS locking to the NFS service fails causing applications like mail to hang. • A potential security vulnerability has been discovered, 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 418.00 OSF400-416	**Patch:** who Command Correction **State:** New patch This patch fixes a problem that occurs when more than 140 users are logged on to a system and the who command is issued. If the output from the command is redirected or piped, the last several lines become corrupt.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 423.00 OSF400-422	**Patch:** named Correction (SSRT0296U, SSRT0494U) **State:** Supersedes patches OSF400-189 (203.00), OSF400-189B (296.00), OSF400-189B-1 (296.01), OSF400-313 (323.00) This patch corrects the following: • A potential security vulnerability has been discovered in BIND (Domain Name Service), where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability. • Corrects a problem where, if the FLAG bit is set in the IP header, screend incorrectly reports: ACCEPT: Not first frag, off 64 • 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 424.00 OSF400-423	**Patch:** Token Ring Transmission Timeout **State:** Supersedes patch OSF400-136 (136.00) This patch corrects the following: • Fixes a Token Ring transmission timeout. The driver can experience "ID 380PCI20001 (8/13/95)" as described in the TI380PCI Errata. • An upgrade/replacement for the Token Ring driver. This patch fixes an intermittent kernel memory fault problem. To ensure data integrity, additional enhancements to transmit and receive list processing routines have also been added.
Patch 425.00 OSF400-424	**Patch:** rdist Utility Correction **State:** New patch Fix for rdist utility to prevent segmentation fault.
Patch 428.00 OSF400-427	**Patch:** Security, (SSRT0490U) **State:** New patch 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 429.00 OSF400-428	**Patch:** Security (SSRT0448U,SSRT0452U) **State:** Supersedes patch OSF400-167 (167.00) 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.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 430.00 OSF400-429	**Patch:** Security, rpc.pcnfsd (SSRT0396U) **State:** Supersedes patch OSF400-023 (23.00) 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. • Provides the following bug fixes and performance enhancements: – When signals causing pcnfsd to terminate or when a SIGPIPE signal was not caught, pcnfsd would exit without producing a core file. – The pcnfsd authentication would cause crashes and memory corruption.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 434.00	**Patch:** Various Terminal Handling Patches
OSF400-433	**State:** Supersedes patches OSF400-030 (30.00), OSF400-035 (35.00), OSF400-053 (53.00), OSF400-041 (41.00), OSF400-067 (67.00), OSF400-085 (85.00), OSF400-092 (92.00), OSF400-142 (142.00), OSF400-146 (146.00), OSF400-236 (256.00), OSF400-324 (333.00), OSF400-368 (369.00) This patch corrects the following: • Fixes "kernel memory fault" panics from the kernel malloc() routine when System V FIFOs created via STREAMS and fattach() are in use. • A remote user will kill rlogin or telnet and the server host will have an orphan login process and rlogind or telnetd process in the sleep state indefinitely. This is seen only with Asian tty (atty) or any other hosts which are running c-list rather than STREAMS tty's. • A panic (kernel memory fault) associated with the STREAMS code when stopping layered products. • Prevents delivery of data in subsequent streams messages with one read of a streams pipe. This problem only happens if the read has a message length greater than the length of the first message in the pipe. • A kernel memory fault panic. This panic occurs 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. • Allows a customer-written device driver to return the customer's own local error value. Without this patch, the user process will get EINVAL instead. • A system could hang after Patch OSF400-035 is installed. • Changes the function that pushes a module on the stream so that the device pointer value is set to the value of the device number saved in the stream head instead of incorrectly setting it to zero. • Kernel memory fault panics seen in systems running with clist-based pseudo-ttys. The kernel memory faults occur either during unrelated malloc() calls, or in calls to proc_ref() from ttymodem(). • System causes an "assert_wait" panic and the stack contains streams modules. • Fixes a problem that causes the system to panic with a kernel memory fault or "malloc_audit: guard space corruption" with osr_run as an entry in the stack. • Fixes a problem that occurs when running STREAMS. The system panics with a kernel memory fault in either osr_run() or osr_reopen(). • Fixes the problem of a system hang due to corruption of a STREAM synchronization queue's forward pointer. The system hangs in the csq_cleanup() function. • Fixes a problem that occurs on an SMP system when running STREAMS. The system panics with the following error message: "kernel memory fault"

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 435.00 OSF400-434	**Patch:** csh Command Correction **State:** Supersedes patch OSF400-193 (206.00) This patch corrects the following: • Corrects several serious problems with the "csh" command. Some of these problems can cause the "grep" and "find" commands to fail, when the user runs the commands under the "csh" shell. • Fixes a problem that occurs when using the C shell (csh). When a command that does both wildcard expansion and command substitution is run in csh, incorrect results are produced.
Patch 436.00 OSF400-435	**Patch:** ksh And sh Corrections **State:** Supersedes patches OSF400-002 (2.00), OSF400-002-1 (2.01), OSF400-002-2 (2.02), OSF400-118 (118.00), OSF400-169 (169.00), OSF400-157 (157.00), OSF400-234 (253.00), OSF400-270 (285.00), OSF400-304 (316.00), OSF400-326 (335.00) This patch corrects the following: • Fixes a problem that occurs if the kernel tunable variable "old-obreak" is set to zero and the system is running the Korn shell (ksh). The shell gets caught in an infinite loop printing a message similar to the following. Eventually the process will core dump. adp/bin/adpbkup[135]: no space • Fixes the following problem. If an attribute has been set to "read-only", and it cannot be set back (unset) to "read/write" status by using the built-in command typeset of the ksh (eg. typeset +r). • 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. This occurred after a user logged into an ULTRIX system from an OSF/1 system using the telnet or rlogin commands. • 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 been set in ksh. • Fixes a problem with the ksh shell program. ksh prevents a command which runs in a sub-process from writing to a tape device. • Fixes a problem in which the ksh command periodically prints erroneous characters instead of the command that was typed. • Fixes a problem in which the ksh shell sometimes reverses the group id (GID) and the effective group id (egid) of the calling process. • Fixes problems that occur when using the ksh shell. When the PATH for a command is not found, the following error message is displayed. Also, when the set command is executed, the system core dumps. /bin/ksh: invalid multibyte character • Fixes a problem that occurs when using the Korn shell (ksh). Variables set with the typeset -L[n] built-in command do not work correctly when other subshells are spawned.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 439.00 OSF400-438	**Patch:** Segfaults In nm For C++ Compiler Correction **State:** New patch This patch fixes segfaults in nm for object files generated by the C++ compiler.
Patch 440.00 OSF400-439	**Patch:** Default C Compiler Correction **State:** New patch This patch fixes a problem that occurs when the default c compiler is used to compile a program using the following switches on the command line: -c -compress -fast
Patch 443.00 OSF400-443	**Patch:** chfsets Function Correction On AdvFS Systems **State:** New patch This patch fixes a problem that occurs on AdvFS systems. The chfsets function returns incorrect exit values and inappropriate error messages.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 446.00 OSF400-448	**Patch:** Library Corrections, (SSRT0425U) (SSRT0296U) **State:** Supersedes patches OSF400-007 (7.00), OSF400-017 (17.00), OSF400-022 (22.00), OSF400-024 (24.00), OSF400-025 (25.00), OSF400-027 (27.00), OSF400-037 (37.00), OSF400-047 (47.00), OSF400-039 (39.00), OSF400-070 (70.00), OSF400-076 (76.00), OSF400-080 (80.00), OSF400-083 (83.00), OSF400-088 (88.00), OSF400-093 (93.00), OSF400-101 (101.00), OSF400-106 (106.00), OSF400-119 (119.00), OSF400-131 (131.00), OSF400-133 (133.00), OSF400-139 (139.00), OSF400-143 (143.00), OSF400-153 (153.00), OSF400-154 (154.00), OSF400-189 (203.00), OSF400-195 (208.00), OSF400-210 (223.00), OSF400-226 (243.00), OSF400-064 (64.00), OSF400-227 (246.00), OSF400-239 (259.00), OSF400-241 (261.00), OSF400-261 (277.00), OSF400-284 (295.00), OSF400-293 (302.00), OSF400-302 (312.00), OSF400-307 (315.00), OSF400-331 (339.00), OSF400-331-1 (339.01), OSF400-323 (332.00), OSF400-334 (340.00), OSF400-341 (345.00), OSF400-348 (354.00), OSF400-362 (363.00), OSF400-372 (377.00), OSF400-393 (389.00), OSF400-400 (392.00), OSF400-402 (393.00), OSF400-403 (397.00), OSF400-408 (400.00), OSF400-410 (396.00), OSF400-410B (407.00), OSF400-417 (482.00), OSF400-430 (431.00) This patch corrects the following: • Fixes a problem with the DECthreads "legacy" library. Specifically, this patch addresses the potential hang of programs that use the Draft 4 interface for pthread_once(). • Fixes a problem in which multithreaded applications that reference a pthread_mutex_destroy routine may fail with EBUSY or the application may hang. • Fixes a problem whereby mkpasswd fails for /etc/passwd files that are very large (containing roughly 30 thousand to 80 thousand entries). • Fixes a problem with the mkpasswd command. Hashed password database files (for example, /etc/passwd.pag and /etc/passwd.dir) are deleted before new database files are created. • Fixes problems in threaded applications with incorrect signal behavior and thread creation failures using user allocated stacks. • Fixes problems that might cause threaded programs running under DIGITAL UNIX 4.0 to hang. Specifically, this patch addresses situations related to DECthread bugcheck, pthread_once() or cma_once(), and unhandled exceptions. • Fixes problems in threaded programs related to DECthreads bugchecks, fork() fork(), stack corruptions and exception handling problems. This patch may also fix problems with non-threaded program relating to exception handling. • 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. • Prevents gethostent() from returning all YP or bind served entries. • Multithreaded programs running on a multiprocessor may behave as if they have fewer CPUs available for execution. A considerable performance degradation can be observed in some cases.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 446.00 continued	• Some valid programs compiled with IEEE mode to receive a floating-point exception even though they should run to completion. • inet_makeaddr() routine in libc that was returning 8 bytes instead of 4. • Math library functions not returning the correct NaN value as defined in the Alpha AXP Architecture Reference Manual (Second Edition). • 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. This problem occurs after a user logs into a system with an SRV4-style LAT device. • Deadlocks that may occur in multithreaded applications which make concurrent use of the fork() and fclose() functions, or the getenv()/setenv() and any time-related function (e.g., localtime()). • Memory leaks with heavily threaded applications using NIS services for passwd, group, and other system database files. • Memory leaks with heavily threaded applications using NIS services for passwd, group, and other system database files. • On systems running DECthreads: Computations that depend on rounding a floating point value to its nearest integer equivalent will receive an integer with the decimal point value truncated. • The filename pattern-matching behavior of the find command when it includes the "?" metacharacter. • The incorrect parameter type declaration in the new swscanf() routine. • Unsuccessful attempts to su to root were not recorded in the syslog/auth.log file, for BASE security. • A memory leak problem associated with the strxfrm() and wcsxfrm() functions. • Compiling under DEC C++ - Reported by our customer SYBASE. • Using fork() in a multithreaded environment. • Generating core files in a multithreaded environment. • Extra signals delivered in multithreaded programs. • Behavior of TIS mutex lock operations. • The interaction of signals with setjmp/longjmp called repeatedly in a loop was causing a segmentation violation and core dump in a customer's application. full IEEE math support. • Threaded applications seeing a deadlock with fork(), premature stack overflows, corrupted mutexes, orphaned condition variable or mutex blocking structures • Fixes a deadlock problem that may occur with multithreaded applications calling any of the functions for getting system database information (gethostent, getservent, etc.) and which also call fork. The deadlock may occur when such applications are run on systems configured to use YP services.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 446.00 continued	• Older call_shared FORTRAN applications to find missing symbols in libc.so. • A potential security vulnerability has been discovered, where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability. • Fixes a problem where a call to popen() hangs after a bad call to pclose() in a threaded program. • Fixes a problem in which mallopt(M_MXFAST), instead of making malloc() faster makes it as much as 65 times slower. • Fixes problems with redundant close operations on file descriptors by Network Information Services (NIS) and Remote Procedure Calls (RPC) in multithreaded applications. • Fixes a problem where conversion from double-precision floating point numbers to single-precision floating point numbers may not round properly in IEEE mode when the result should be the smallest denormal. • Fixes a problem with fastmath functions F_Exp() and F_Pow() that would cause floating exception core dumps. • Fixes a problem in which the rcmd function may cause the system to dump core. • Fixes the following two problems that occur in the DECthreads core library: – The process blocked signal mask, as set by sigprocmask(), cleared in the child process following a fork(). – Under certain load conditions, a DECthreads bugcheck occurs in pthread_kill(). This results in a core dump. • Allows customers to create hashed passwd databases from large passwd files by using a new option (-s) to the mkpasswd command. The -s option increases the block size of the database page file. • Fixes a TCP/IP problem that can occur with programs linked with the libc library. These programs may return a value of (-1) when calling the svc_tcp() function. • Fixes a deadlock issue between fork() processing and exception handling on DIGITAL UNIX 4.0. An exception occuring during a fork() operation would cause the child and parent processes to hang with no cpu activity. • Fixes a problem in libc. The allocation of pty's sometimes doesn't work correctly. This can cause problems with the EMACS editor. • Fixes a couple of problems in the mkpasswd command. • Fixes a problem with fastmath functions F_Exp() and F_Pow() that would cause floating exception core dumps. • This patch fixes two problems in the DECthreads library: – On multiprocessor platforms, condition variable broadcasts were occassionally being lost. – Stack unwinding during exception processing was losing contexts, resulting in incorrect stack traces.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 446.00 continued	• Fixes a problem that may cause a program to cause the IEEE floating point emulator to emit this message: FATAL IEEE FLOATING POINT EMULATION ERROR: • Corrects a problem related to the statically initialized mutexes in DECthreads library (libpthread.so). • Fixes a problem whereby a call to the libc dbm_open() routine followed immediately by a call to dbm_close() causes hashed database directory files to be truncated. • Corrects a problem which occurs when pthread_cond_timedwait() is called with a large timeout value (greater than 23 days). There is a problem in the Bind 4.9.3 patch which may cause incorrect messages to be reported. It may also cause statically linked programs using certain network functions in libc to core dump. • Fixes a problem with call_shared executables that are linked with libc.a instead of libc.so. A symptom of this problem is that routines like dlopen(3) and __fini_* routines are not run. • Fixes a problem with the auditd daemon. If auditd is logging to a server and the server becomes unavailable, the CPU usage for the daemon rises dramatically. • Fixes a problem in which RPC client functions do not correctly handle system calls interrupted by a signal (EINTR errors). • Fixes two kernel memory faults in networking code. • Fixes a problem that causes the readdir_r() function to read past the end of its input buffer.
Patch 453.00 OSF400-455	**Patch:** lex Command Correction **State:** New patch This patch fixes a problem with the lex command. Programs built with lex may exhibit various problems which only occur after the following warning: Maximum token length exceeded

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 455.00 OSF400-457	**Patch:** pax tar And cpio Archive Handling Correction **State:** Supersedes patches OSF400-258 (274.00), OSF400-320 (329.00), OSF400-374 (383.00), OSF400-391 (484.00), OSF400-395 (485.00) This patch corrects the following: • Fix pax's tar and cpio archive handling to allow filesizes greater than 4GB. • Fixes a problem with the tar "tv" command in reporting ownership on a file that had no legitimate owner at the time it was archived. Based on the position of the file in the archive, tar returned the owner of a previous file, or the values -973 for userid and -993 for groupid. • Fixes problem in which /usr/bin/pax : cpio -pl does not link files when possible, but copies them. • Fixes a file corruption problem that may occur with certain applications, for example Realtime applications, that use the plock() system call or the mlock() and mlockall() library routines. • Fixes the following problems with the pax command when cpio format is used: – The cpio -z command hangs the system when small files are read using a large block size. – When reading a series of commands, cpio fails on the second command and displays a "No input" error message. If an identical third cpio read is issued, cpio works as expected. • Fixes a problem with the tar and pax programs. These programs incorrectly append files to an existing archive and cause the file to become corrupt.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 462.00 OSF400-464	**Patch:** ATM Corrections **State:** Supersedes patches OSF400-018 (18.00), OSF400-040 (40.00), OSF400-059 (59.00), OSF400-072 (72.00), OSF400-078 (78.00), OSF400-084 (84.00), OSF400-102 (102.00), OSF400-138 (138.00), OSF400-219 (237.00), OSF400-253 (269.00), OSF400-286 (307.00), OSF400-288 (299.00), OSF400-411 (413.00), OSF400-425 (426.00), OSF400-432 (433.00), OSF400-288 (299.00), OSF400-411 (413.00), OSF400-425 (426.00), OSF400-432 (433.00) This patch corrects the following: • Fixes problems in the error paths of the ATM subsystem. A majority of these result in system crashes. These crashes are most prevalent when stressing LAN Emulation (LANE). • The system fails to establish one of the required VCs when joining an ATM Emulated LAN (LANE). • A panic and other problems that can occur in the ATM subsystem when there is a large amount of signalling activity. It also fixes a potentially invalid signalling message. • The ATM LAN Emulation code which was preventing correct emulation of Ethernet Multicast functionality. • A panic when the ATM driver is brought up/down and Lan Emulation (LANE) is active. A lockmode=4 (lock debug mode) panic is also fixed. Both of these are a by-product of installing patch OSF400-040. • A number of kernel memory fault panics in the ATM subsystem. The panics are seen when the connection to the ATM switch is lost, particularly under heavy load. The patch also fixes problems with ATM timers and memory leaks. • ATM issues relating to the use of UNI 3.1 signaling. • ATM issues relating to running LANE (Lan Emulation). • Systems with a high rate of connection startup/teardown may panic in atm_arp_timer() with "kernel memory fault". • Systems running ATM in multivendor environments can panic in atmip_send() with "kernel memory fault". • The atmarp hostname command may return without printing out the contents of the ATM ARP entry for the hostname. • Two panics in the lta driver, ATM LANE interoperability problems with IBM switches and slow recovery of UNI 3.0 signalling from network interruptions. • An upgrade/replacement for the OTTO/OPPO ATM driver and fixes a number of flow control and signalling problems. If you are seeing "No Buffer Space" messages, experiencing pauses or hangs when receiving data on signalling/ ilmi pvc's, or have any problems with FLOWMASTER flow control with CLIP or LANE over ATM, you should install this patch. • Contains performance enhancements to the ATM OTTO driver when greater than 300 VC's are configured. This replacement driver uses hash buckets to improve search time in the VC data structures resulting in significant performance gains. • When tcpdump is run with ATM LAN emulation, a kernel memory fault occurs.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 462.00 continued	• Fixes two problems with the ATM 350 driver. On reboot, a panic could be encountered before getting into single user mode. The panic would occur inside the ltaintr routine and this routine would be noted in the dump stack trace. This problem was seen on Personal Workstation 500ua (MIATA) and the ATM 350 card. The second problem is a panic: thread_block: interrupt level call when rt_preempt_opt (REALTIME preemption) is enabled. A typical stack trace would look like this for the top of the stack: panic thread_block() thread_preempt() panic thread_block() unix_release_force() unix_release() schedtransmit() softclock_scan() or this: panic thread_block() thread_preempt() panic thread_block() unix_release_force() unix_release() ottooutput() atm_cmm_send() • An upgrade enhancement to the ATM350 driver. This patch prevents panics in driver routines that can be called from different interrupt levels. • Fixes a problem with the ATMworks 351 (Meteor) loadable driver.
Patch 463.00 OSF400-465	**Patch:** LSM volsave Command Correction **State:** New patch This patch fixes a problem with the LSM volsave command. The volsave command returns an exit status of 1 (failure), even when the LSM configuration is successfully saved.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 465.00 OSF400-467	**Patch:** Upgrade For "FTA" FDDI Driver To Fix DMA Error **State:** Supersedes patches OSF400-225 (242.00), OSF400-409 (399.00) This patch corrects the following: • An upgrade/replacement for the "FTA" FDDI driver and fixes a DMA Error which can occur with the older driver. If it became necessary to back out a partially constructed frame from the transmit queue, the older driver was unable to properly backed out the frame before restarting. This resulted in the following errors being logged to the /var/adm/messages file: vmunix: fta0: Halted. vmunix: fta0: Halt Reason: DMA Error vmunix:: fta0: Link Unavailable. vmunix: fta0: Link Available. • Fixes a problem that may occur on systems with a FDDI controller. During system boot, the system may panic with a message similar to the following: panic (cpu 8): kernel memory fault • Fixes a kernel memory fault caused by the fta FDDI driver.
Patch 466.00 OSF400-468	**Patch:** dtterm Displays All Characters in PC Codeset IBM-850 **State:** Supersedes patch OSF400X11-023 (501.00) This patch corrects the following: • Provides a new en_US.cp850 locale for processing text data originating from the PC environment. • Provides the ability to let dtterm display all the characters in the PC codeset IBM-850.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 468.00 OSF400-470	**Patch:** syslogd Correction, (SSRT0482U,SSRT0521U) **State:** Supersedes patches OSF400-019 (19.00), OSF400-019-1 (19.01), OSF400-031 (31.00), OSF400-032 (32.00), OSF400-048 (48.00), OSF400-050 (50.00), OSF400-052 (52.00), OSF400-054 (54.00), OSF400-055 (55.00), OSF400-057 (57.00), OSF400-062 (62.00), OSF400-082 (82.00), OSF400-094 (94.00), OSF400-098 (98.00), OSF400-099 (99.00), OSF400-100 (100.00), OSF400-110 (110.00), OSF400-113 (113.00), OSF400-114 (114.00), OSF400-121 (121.00), OSF400-123 (123.00), OSF400-127 (127.00), OSF400-129 (129.00), OSF400-141 (141.00), OSF400-165 (165.00), OSF400-161 (161.00), OSF400-163 (163.00), OSF400-180 (194.00), OSF400-185 (199.00), OSF400-197 (210.00), OSF400-200 (212.00), OSF400-202 (214.00), OSF400-213 (229.00), OSF400-208 (221.00), OSF400-056 (56.00), OSF400-198 (211.00), OSF400-212 (228.00), OSF400-216 (232.00), OSF400-220 (238.00, OSF400-221 (239.00), OSF400-224 (241.00),OSF400-201 (213.00), OSF400-021 (21.00),OSF400-012 (12.00), OSF400-096 (96.00), OSF400-108 (108.00), OSF400-145 (145.00), OSF400-181 (195.00), OSF400-182 (196.00), OSF400-186 (200.00), OSF400-232 (251.00), OSF400-233 (252.00), OSF400-242 (264.00), OSF400-244 (266.00), OSF400-235 (255.00), OSF400-010 (10.00), OSF400-247 (267.00), OSF400-250 (268.00), OSF400-237 (257.00), OSF400-245 (265.00), OSF400-130 (130.00), OSF400-262 (278.00), OSF400-266 (281.00), OSF400-271 (286.00), OSF400-240 (260.00), OSF400-287 (298.00), OSF400-289 (300.00), OSF400-294 (303.00), OSF400-296 (305.00), OSF400-298 (310.00), OSF400-351 (222.00), OSF400-273 (288.00), OSF400-281 (292.00), OSF400-283 (361.00), OSF400-308 (319.00), OSF400-316 (326.00), OSF400-335 (341.00), OSF400-342 (346.00), OSF400-346 (358.00), OSF400-353 (359.00), OSF400-354 (360.00), OSF400-356 (365.00), OSF400-357 (367.00), OSF400-360 (381.00), OSF400-363 (391.00), OSF400-367 (368.00), OSF400-049 (49.00), OSF400-104 (104.00), OSF400-147 (147.00), OSF400-229 (248.00), OSF400-369 (366.00), OSF400-373 (390.00), OSF400-378 (388.00), OSF400-384 (384.00), OSF400-394 (387.00), OSF400-397 (401.00), OSF400-407 (398.00) OSF400-407B (408.00), OSF400-388 (409.00), OSF400-389 (481.00), OSF400-414 (416.00), OSF400-418 (420.00), OSF400-420 (421.00), OSF400-421 (422.00), OSF400-431 (432.00), OSF400-441 (441.00), OSF400-442 (442.00), OSF400-446 (445.00), OSF400-451 (449.00), OSF400-452 (450.00), OSF400-456 (454.00), OSF400-458 (456.00), OSF400-459 (457.00), OSF400-461 (459.00), OSF400-466 (464.00), OSF400-469 (467.00) This patch corrects the following: • Fixes a problem in which network applications communicating to one of the host's own addresses, may hang, or receive the error message: no buffer space available The problem occurs due to a queue full condition on the interface. • This network patch, which greatly improves DIGITAL UNIX networking performance, is targeted at high traffic Web server systems or any system which handles a large number of TCP connections simultaneously, i.e., more than several thousand at one time. • This patch addresses compilation errors in the header file for C and C++ programs.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 468.00 continued	• Fixes a problem with the fsck command. When fsck is run on a non-existent file system or on a currently mounted file system, it returns a success status of zero. It should return a non-zero status. • Fixes a problem that occurs on AlphaServer 8200 systems running a firmware revision prior to 3.9. The pset_info and psradm commands may fail to correctly report that a CPU is shut down. • 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. • This patch resolves a TCP/IP network hang due to IP Q ACK deadlock. When this condition occurs the IP Q becomes full due to saturation. Representative console messages indicating this condition are shown below: SIS00-00-root: IP q full, 315617 packets dropped in the last 5 mins. • Fixes a performance problem that occurs with UFS file systems. • Fixes a problem in which the system can panic with "lock already owned by thread". • Fixes ICMP REDIRECTS. When an ICMP REDIRECT is received, the routing table was updated properly, but the IP layer didn't use the new route information. • Fixes a problem that occurs on all systems that use networking services. • Fixes a system panic caused by Windows95 or WindowsNT systems sending an illegal length ping (ICMP)packet. • A kernel memory fault panic that occurs in ip_forward. • TCP connections may hang and eventually time out if IP options are in use. • Datagram loss when real-time preemption is turned on. • 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. This patch is MANDATORY to install. • Fixes a kernel memory fault in ether_output packet filter, when running tcpdump. • Fixes problems encountered when using signals with multithreaded programs. • Fixes a problem in which the ufs property list can become corrupted. • The kernel panics with a "kernel memory fault", typically in either the vm_pg_alloc() or vm_zeroed_pg_alloc() routines. • This patch corrects a problem with the exec() system function. A shell script that has "#! " as the first line of the script, invokes the program but does not set the effective user id for the execution of the program.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 468.00 continued	• Fixes a problem that occurs in the vm subsystem. The system panics with "PANIC: VL_UNWIRE: PAGE IS NOT WIRED" message. This panic occurs most frequently on systems running database applications. • When compiling a C++ program, an error message like the following is returned: cxx: Error: toto.cc, line 9: In this statement, "_Plocaltime_r" is not declared The interface given in the error message will always begin with _P and end with _r. • The interface given in the error message will always begin with _P and end with _r. • Fixes a problem that occurs when the system panics with the following error message: kernel memory fault • Allows tuneablity for existing two level task swapping scheme. • Provides support for the fuser utility. This utility displays a list of processes that are holding references to a file on the file system that cannot be unmounted. • The ObjectStore application from Object Design, Inc. fails with the following error: "Fatal error Invalid argument(errno = 22) munmap failed: cl_mmap:" • This patch resolves a kernel memory fault. This patch is MANDATORY to install. • Fixes a problem that occurs when running the NetWorker Version 4.2c application. Without this patch, NetWorker Version 4.2c will not perform well. • The user or system UAC_NOPRINT settings are ignored when an unaligned access trap on a user address was taken while in kernel mode; the unwanted error message is still printed. • This patch corrects a problem in which the system can panic when a ufs-mounted floppy is removed from the drive, then replaced and accessed. • Fixes kernel asynchronous I/O (AIO) problems that occur on clustered systems and systems using major databas products on raw disk partitions. Users of database products are advised to install this AIO patch. • Fixes system crash when setting the date on SMP systems. • Fixes a network socket problem with select() missing state changes on clients from non-write to writable. • This is a mandatory patch for the following systems: – Systems that use program debuggers such as Ladebug, dbx, TotalView, or gdb – Systems that use the /proc file system in any other way (for example, the System V Environment ps command) – Systems that experience panics in the /proc file system – Systems that panic when running multithreaded programs that call an exec() function

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 468.00 continued	• System panics with message: "vm_map_swapout: negative resident count". • vmstat(1) command displays negative numbers when used with the '-P' option. Problem may not appear on all platorms / configurations. It is dependent on how the system constructs various internal data structures. • Fixes "kernel memory fault" panics from the kernel malloc() routine, and threads hanging in vfs_busy() when file-on-file mounting (kernel option FFM_FS) is used with fattach()/fdetach() or System V STREAMS. • System hangs and crashes in CAM that can occur when running HSZ40/50/70s. • System panics after creating a symbolic link to the root file system ('/') and accessing it like a normal file. For an AdvFS file system, the system will panic with the following error message: bs_bf_htop: invalid handle For other file systems, the system will panic with the following error message: vrele:bad ref count • Prevents a "kernel memory fault" in bread() during sync operations. • Processes can hang waiting for a system call to table() to complete. • When Fortran programs or multithreaded applications that were built on a DIGITAL UNIX V3.2C system are run on a DIGITAL UNIX V4.0 system, the system displays the following error message: msg_copyout: map entry limit reached • The /proc filesystem panics with either a "kernel memory fault" or "thread_block: simple lock owned" message. This patch also improves the behavior of the Ladebug debugger. • Hangs that can occur during the "syncing disks..." portion of panic processing, improves the reliability of getting a dump after a system panic, and also makes it more likely that AdvFS buffers will be synced to disk after a system panic. • The system will panic with "u_shm_oop_deallocate: reference count mismatch." • May improve the performance of a multithreaded application (for example, a video server) that experiences heavy I/O.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 468.00 continued	• Prevents duplicate namecache entries on SMP systems. • Multiprocessor systems using the AdvFS file system, particularly systems also using AdvFS for the root and usr file systems, may experience intermittent freezing of interactive processes when the system has a moderate to heavy I/O load. The freezing of interactive processes may last from a few seconds too many minutes but will eventually return to normal. This problem may also occur on multiprocessor systems using the NFS client or graphics sub-systems. • Calls to flock() can hang a process on an SMP system if 2 or more processes are attempting to obtain and release an flock() on the same file. • Processes hang in an uninterruptible state on a machine which uses NFS loopback mounts. • 'no sense' and 'unit attention' events are being logged in the error log file as actual errors (CAM_ERROR packet types) when they should be logged as informational (CAM_INFORMATIONAL packet types). • A kernel memory fault panic that occurs on SMP platforms when running the Unicenter product from Computer Associates in conjunction with Oracle software. • The system panics with the message "panic (cpu #): kernel memory fault". • setsockopt(), getpeername(), or bind() will fail with EINVAL if the socket is in a shut down state. In particular, AF_X25 sockets using setsockopt() with the XSO_CLEARCALL option, and AF_WAN sockets using setsockopt() with the HDLC_CLOSEPORT option, can experience this problem. • Object Broker 2.6-07. Object Broker fails with the following message: Dynamic load of component 'OrbV12' for subsytem "Agent" failed. The specified executable for the method could not be dynamically loaded. • A call to the mmap routine returns success without actually mapping the memory region. Subsequent access to the memory region will generate a segmentation fault. • FORTRAN application fails with "Cannot map data". • FORTRAN application fails with "Could not open message catalog". • Provides additional event logging by the SCSI/CAM disk driver to the binary.errlog file. • Fixes a panic that prints "kernel memory fault". • Corrects a problem with an NFS V3 mounted AdvFS file system where under heavy I/O load, data being written to a file may be lost. Additionally, because file stats are not being saved, the file modification time may revert to a previous value. • Fixes a panic occurs when a UNIX domain socket lock is being held while calling vrele(). • Fixes a 'recursion count overflow' problem that occurs on DIGITAL UNIX systems.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 468.00 continued	• An enhanced fix to the solockpair() routine. This fix was needed because the routine was freeing a socket lock structure that was concurrently spun upon in lock_write(). Typical problem symptoms include kernel memory faults with sockets, mbufs and mblocks as well as hangs. Applications using sockets in a multithreaded, multicpu environment can experience a number of lock violations with the socket structures. This patch is MANDATORY to install on all systems. It will be effective on Uniprocessor systems when lockmode debugging is invoked. • Allows some third-party NFS v2 clients to experience a performance improvement. • Fixes a problem that occurs when using real-time applications. When writing large (sequential) files to a UFS file system, time constraints associated with the application may be violated. • Greatly reduces the number of "NFS stale file handle" messages logged to an NFS server system console. • This is a mandatory patch for the following systems and conditions: – Systems that use program debuggers such as TotalView, Ladebug, dbx, or gdb. – Systems that use the /proc file system in any other way (for example, the System V Environment ps command) – Systems that experience panics and hangs in the /proc file system. – Systems that panic when running multithreaded programs that call an exec() function. • Fixes a problem with the "ifconfig -a" command. At times, the command will not display all of the network interfaces. • Adds a mechanism to the poll() system call to allow it to be used as a timer. • Fixes a problem related to misinterpretation of multibyte characters by diff command. The problem also affects the delta command of SCCS. The symptom of the problem in the diff command is that it sometimes treats a text file containing multibyte characters as a binary file. The symptom of the problem in the delta command is that it sometimes fails to check in a program source file containing multibyte characters. • Eliminates panics that will occur when attempting to execute shell scripts on a filesystem mounted with the "noexec" option. • Fixes a problem in which a system hang or core dump occurs when one program inadvertently overwrites the contents of another program. • System experiences simple lock timeout panics in virtual memory routines when free memory is short and system is trying to reclaim memory. • A potential security vulnerability has been discovered, where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability. • Fixes a problem in which a system may crash if multiple bad blocks on a SCSI device are encountered simultaneously.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 468.00 continued	• Fixes several problems in the vm subsystem: – Processes using shared memory (SSM) may hang. – Skewed swap space is not allocated evenly. – Skewed swap space is not allocated evenly. • 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. • 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. • 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 the problem of audit_tool terminating prematurely the reading of a complete large log file via zcat. This usually occurs under gui control. • This is a mandatory patch for SMP systems with AdvFS file systems. Fixes a performance degradation problem that may occur. • Fixes a problem that may occur after a system panics. The system may hang when trying to do a crash dump. • This is a mandatory patch for AlphaServer 2000 and AlphaServer 2100 SMP systems. This patch fixes the following problems: – Internal lockups may cause performance degradation. – The system clock may lose time. • Fixes a panic with the panic string "spec_badop called" that can sometimes occur when an fpathconf system call is issued for a file in an ADvFS filesystem. The panic has following stack trace: panic (s = "spec_badop called") spec_badop fpathconf syscall _Xsyscall • Probe of isp fails intermittently during boot. • A problem that occurs with the Qlogic driver. Because of a problem with the sim code, command timeouts occur and the printer device will not be detected during SCSI device configuration.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 468.00 continued	• ISP1020 driver corrections: – 'minimum spl violation' panics with lockmode=4. – simple lock time limit exceeded panics. – 'CAM_ERROR entry too large' messages. – 'Unable to restart Qlogic(LUN queue after abort)' panics. – Probe of isp fails intermittently during boot. • A number of problems have been fixed by this patch of the simport driver: – 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 3 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" • Provides general support for Version A11 KZPSA firmware. • Improves the performance of applications that map hundreds of thousands of files into the virtual address space. • Fixes a problem in which a filesystem cannot be unmounted. The system displays a "Device busy" error message. • Fixes a problem that occurs when starting up a system that is running the auditing subsystem and the performance manager. The system panics with the following error message: kernel memory fault • This patch is MANDATORY. This patch contains two vm fixes in both the UFS and NFS code that collectively resolve a multitude of nfs and nfsd hangs. • Corrects a raw I/O data corruption problem that occurs when using database applications. The problem is seen when the new-wire-method is active. • Back-port of PTMIN-style multioption kmem_debug settings. Changed all-or-one kmem_debug bucket selection to all-or-as-selected. Added two new kmem_debug options, KMEM_DEBUG_LINKS and KMEM_DEBUG_PROTECT. • Fixes a UFS file system problem. The system may panic with the following error message: panic spec_badop called • Eliminates the display of "Stack overflow: pid..." messages that may occur when running Ladebug.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 468.00 continued	• Fixes a potential memory leak problem that occurs when using the KMEM_DEBUG_PROTECT option of the kmem_debug tunable attribute. • This patch is MANDATORY. Resolves an inode locking problem in the UFS iupdat() and itimes() functions. • Fixes a problem in which a file-on-file system mount of either an NFS or a /proc file system will panic the system. • Fixes an AdvFS problem in which the "advfsstat -n" command causes a core dump. The system displays the following error message: Memory fault(coredump) • When a zero length message is sent to an invalid SVIPC message queue, kernel memory is corrupted. • This is a mandatory patch. This patch fixes a problem that occurs on programs that are linked with the pthreads library. After a parent process forks a child process, the child's floating point state may become corrupt. • Fixes a problem in which core() system call would try to dump from a memory region that has no permission, cause an access violation in core() and the core file would be unusable. An example of the problem: % file core core: core dump, core file is incomplete % dbx program core . . . can't attach to loader: I/O error Exiting due to error during startup • Fixes a problem that causes the system to panic with the following error message: u_anon_free: page busy • Fixes a problem with the ufs_fsck. ufs_fsck would mishandle certain dir corruptions,recursively asking the user if they want to fix it. • Fixes a problem that occurs on AlphaServer 8200/8400 systems. The sytem may panic with the following error message: tb_shoot ack timeout • Fixes a problem of memory corruption. A TCP control structure is illegally accessed after it is released. The corrupted memory buckets are the 256-byte size. • Fixes a problem that occurs on AlphaServer 4100 systems. If no devices are attached to the KZPSA disk controller, the system may panic when attempting to perform I/O. • Fixes an AdvFS problem in which the system may panic with the following error message: thread_block: simple lock owned

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 468.00 continued	• Fixes a problem in which the uswitch system call does not work when an application tries to reset the USW_NULLP option. • Fixes a problem with the nfsd daemon. Although the maximum number of threads that nfsd can run is 128, the nfsd daemon will not start when the sum of UDP threads and TCP threads equals 128. • A potential security vulnerability has been discovered, where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability. • Fixes a panic that occurs when the system's message buffer size is increased to beyond the default size of 4096. During the subsequent reboot, the syslogd daemon fails with a "Segmentation fault (core dumped)" message, and creates a core file in the "/" directory.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 470.00 OSF400-473	**Patch:** GEMC Compiler Corrections **State:** Supersedes patches OSF400-091 (91.00), OSF400-149 (149.00), OSF400-187 (201.00), OSF400-257 (273.00) This patch corrects the following: • Fixes a DEC C compiler problem that occurred when compiling a structure tag whose length exceeded 256 characters. • Fixes a problem where the DEC C compiler would hang when compiling files containing many thousands of #line directives. • The compiler generates 8 bytes of return code for functions that are defined to return a 4-byte structure. • The compiler generates 8 bytes of return code for functions that are defined to return a 4-byte structure. • The compiler preprocessor was incorrectly issuing a warning diagnostic on the use of an octal constant. • The compiler was not issuing a diagnostic for the use of the "long double" datatype. • This patch provides a new version of the DEC C compiler to fix QAR 49944. It fixes a problem that causes the compiler to generate incorrect code for switch statements whose expression is of type short or type char. • Fixes three DEC C compiler problems. – Fixes "Assertion failure: Compiler internal error" compiler crash that occurs when compiling xemacs. – Fixes "Invalid expression" error with valid token-pasting macro. – Fixes "Fatal: memory access violation" compiler crash when the left side of a structure pointer operator (->) was not an lvalue. This case should produce a compiler error. • Fixes the following problems: – A compiler code generation problem that caused incorrect code for a left shift on a signed int when compiled in ANSI (-std or -std1) compilation modes. – A problem where a structure return temporary is not preserved until later used in an enclosing funtion call; originally reported in the comp.UNIX.osf.osf1 newsgroup. – A "GEM ASSERTION, Compiler internal error" problem when compiling a complex conditional expression with -O0.
Patch 474.00 OSF400-478	**Patch:** LAT Correction **State:** Supersedes Patch OSF400-107 (107.00) This patch corrects the following: • Corrects a problem where processes such as wall, ntalkd, and comsat, when associated with LAT devices, get stuck in the 'u' state (processes are hung) and cannot be cleared from the system. • When printing using DIGITAL UNIX LAT (V4.0 or later) to a printer connected to a PC running Pathworks, "I/O error" is displayed and nothing is printed.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 475.00 OSF400-479	**Patch:** Corrects STREAMS TTY Line Discipline **State:** Supersedes patches OSF400-173 (173.00), OSF400-312 (321.00) This patch corrects the following: • The STREAMS tty line discipline not correctly processing type ahead characters. Also this patch fixes a delay in closing the STREAMS tty line discipline (typically seen on LAT connections). • Fixes a wide variety of system panics and other problems caused by random memory corruption. • Fixes a problem when printing to slow printers using DIGITAL UNIX LAT. The end of a large file fails to print and no error is reported.
Patch 480.00 OSF400-382	**Patch:** dump And rdump Command Corrections **State:** Supersedes patch OSF400-079 (79.00) 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.
Patch 483.00 OSF400-405	**Patch:** Greater Than 500 XTI Connections Crash Correction **State:** Supersedes patches OSF400-151 (151.00), OSF400-171 (171.00), OSF400-196 (209.00), OSF400-264 (280.00), OSF400-385 (505.00) This patch corrects the following: • Fix for a mutex lock problem in TLI. The problem causes multithreaded TLI applications to block forever. • Fixes the problem of t_optmgmt() T_NEGOTIATE calls returning T_SUCCESS, but not actually negotiating the socket options. This behavior is a UNIX95 specification standard compliance bug. • Fix for a problem that manifests itself by the system hanging or becoming inoperable when a number of XTI connections reaches 500. • Resolves a hang in the xticlose() routine and a kernel memory fault in the xti_discon_req() routine. • Corrects a problem with the xti/streams interface module which could result in a kernel memory fault panic during use by xti application programs. • Fixes a problem with the implementation of the TPI interface. This problem occurs if you are using DIGITAL's XTI libxti library with a third-party (non-DIGITAL) STREAMS driver.
Patch 487.00 OSF400-379	**Patch:** find Command Correction **State:** New patch This patch fixes various problems with the find command.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 488.00 OSF400-396	**Patch:** Security Patch, (SSRT0505U) **State:** Supersedes patch OSF400-144 (144.00) This patch corrects the following: • Fixes a problem with the ftp command. if you ftp to an IBM MVS system using the IP address, the IBM system will refuse the connection. This problem be encountered on any system that validates TOS (Type Of Service) requests if the file /etc/iptos is not used on the client. It is recommended that this patch be installed on all OSF systems. • 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 490.00 OSF400-487	**Patch:** Run-Time Support For DIGITAL C++ V6.0 Compiler **State:** New patch This patch provides the requried run-time support for images created by the DIGITAL C++ V6.0 and above compiler. Contact the DIGITAL C++ compiler group (cxx@lego.zko.dec.com) for details.
Patch 491.00 OSF400CDE-013	**Patch:** Security, (SSRT0498U) **State:** New patch A potential security vulnerability has been discovered in 'libDtSvc', where under certain circumstances users may gain unauthorized access. DIGITAL has corrected this potential vulnerability.
Patch 493.00 OSF400CDE-015	**Patch:** Security, (SSRT0431U) **State:** Supersedes patch OSF400CDE-008 (225.00) 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 494.00 OSF400CDE-014	**Patch:** dtterm Corrections **State:** Supersedes patches OSF400CDE-003 (177.00), OSF400CDE-004 (178.00), OSF400CDE-012 (492.00) This patch corrects the following: • Users appear to be logged in when they are not because CDE dtterm sometimes doesn't reset the utmp entry on exit. • Prevents the escape sequence that sets DECterm window titles from hanging dtterm windows. • When running the Common Desktop Environment (CDE), a dtterm window in which vi is being used can hang when doing a cut and paste operation from a second window. • When running the Common Desktop Environment (CDE), a dtterm window in which vi is being used can hang when doing a cut and paste operation from a second window. • Provides the ability to let dtterm display all the characters in the PC codeset IBM-850.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 495.00 OSF400DX-015	**Patch:** OSF400DX-015 **State:** Supersedes patches OSF400DX-006 (216.00), OSF400DX-009 (272.00), OSF400DX-011 (322.00) This patch corrects the following: • A potential security vulnerability has been discovered, where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability. • Fixes a problem that occurs on DIGITAL UNIX systems running Version 4.0 or higher with C2 security enabled and Patch OSF400DX-006 installed. The dop command rejects all password attempts when run by non-root users. • Fixes a problem that occurs on systems that have installed Patch OSF400DX-006. If more than one argument is given on the dop command line, dop passes all arguments as a single argument to the command. • The startup of nissetup, latsetup and btcreate /etc/doprc entries via the dop command fails with exit code of 2.
Patch 496.00 OSF400DX-013	**Patch:** Account Management Command Correction **State:** Supersedes patches OSF400DX-005 (183.00), OSF400DX-008 (244.00) OSF400DX-010 (289.00) This patch corrects the following: • When creating a new user account with a home directory of root, the permissions on the root directory are changed to 700, rendering the root file system inaccessible to non-root users. Patch Kit-0001 causes a problem with the System V Environment (SVE) /usr/opt/svr4/usr/bin/passwd command. If an invalid password is entered, subsequent invocations of the passwd command, /usr/bin/X11/dxaccounts command, or the account management commands fail with the following error: The password and group files are currently locked by another user. • Fixes for miscellaneous problems with the account management commands, specifically the Account Manager graphical user interface (/usr/bin/X11/dxaccounts) and the command line interface (useradd, userdel, groupadd, etc). • Fixes a problem that causes the account management commands (dxaccounts, useradd, and usermod) to split long NIS group lines incorrectly. This causes a majority of users to have improper access to files, directories, and applications and also causes the newgrp command to fail. • Fixes the following problems: – When Enhanced Security is enabled, the useradd and usermod commands incorrectly set the password expired and password lifetime attributes to 0 when not specified on the command line. – The administrative_lock_applied command line option for useradd and usermod does not correctly lock and unlock an account. – When Enhanced Security is enabled, userdel command incorrectly removes an account from /etc/passwd.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 499.00 OSF400X11-024	**Patch:** X Terminal Logout Correction, (SSRT0422U) **State:** Supersedes patches OSF400X11-003 (186.00), OSF400X11-010 (189.00), OSF400X11-017 (320.00), OSF400X11-021 (403.00), OSF400X11-022 (498.00) This patch corrects the following: • A potential security vulnerability has been discovered in 'libXt', where under certain circumstances users may gain unauthorized access. DIGITAL has corrected this potential vulnerability. • Fixes a problem in which the output of the "last" or "finger" command lists users that are not currently logged in. • A potential security vulnerability has been discovered, where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability. • Fixes a memory leak in Xlib when using fonts in an international (I18N) environment. This problem affects Netscape Navigator in particular. • X programs run by root or installed with suid root core dump on a fatal error such as an invalid display. • When managing a CDE session on an X terminal from a DIGITAL UNIX system, and the X terminal does not perform a normal logout, some of the CDE processes on the DIGITAL UNIX system are left running.
Patch 500.00 OSF400X11-025	**Patch:** Memory Leak In X Server Correction **State:** New patch This patch fixes a memory leak in the X server which is seen on systems with a ZLX-E1, ZLX-E2, ZLX-E3, ZLXp-E1, ZLXp-E2, ZLXp-E3, PowerStorm 3D30, or PowerStorm 4D20 graphics card.
Patch 502.00 OSF400-415	**Patch:** syslogd Correction, (SSRT0499U) **State:** Supersedes patch OSF400-306 (314.00) This patch corrects the following: • Fixes a problem in which the syslogd program cannot properly forward large messages to remote systems. It will either write them to the wrong facility (specified in /etc/syslog.conf) or write incomplete data. • A potential security vulnerability has been discovered, where under certain circumstances, system integrity may be compromised. This may be in the form of improper file or privilege management. DIGITAL has corrected this potential vulnerability.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 503.01 OSF400-489	**Patch:** AdvFS Patches **State:** Supersedes patches: OSF400-001 (1.00), OSF400-045 (45.00), OSF400-068 (68.00), OSF400-111 (111.00), OSF400-105 (105.00), OSF400-148 (148.00), OSF400-125 (125.00), OSF400-176 (191.00), OSF400-176-1 (191.01), OSF400-217 (234.00), OSF400-228 (247.00), OSF400-239B (294.00), OSF400-231 (250.00), OSF400-259 (275.00), OSF400-122 (122.00), OSF400-297 (309.00), OSF400-254 (270.00), OSF400-315 (325.00), OSF400-322 (331.00), OSF400-344 (356.00), OSF400-399 (486.00), OSF400-413 (415.00), OSF400-436 (437.00), OSF400-445 (444.00), OSF400-449 (447.00), OSF400-474 (471.00), OSF400-476 (472.00), OSF400-482 (478.00), OSF400–489 (503.00) This patch corrects the following: • Fixes two problems that occur on AdvFS systems: – An AdvFS data corruption problem can occur in user files. This problem will not produce either a core file or return non-zero system codes when accessing the corrupted file. – The verify command does not detect corrupted files. • Multithreaded applications that call the pthread_mutex_destroy routine may fail when there are no threads referencing the mutex. This is caused by a condition inside the pthread_mutex_unlock code. The typical symptom will be a return value of EBUSY from pthread_mutex_destroy. • Fixes a problem with AdvFS in which the following two panics occur: AdvFS Exception Module = 1, line = 1891 kernel memory fault • Systems running with AdvFS and LSM under heavy I/O loads can have sluggish interactive performance. In a DECsafe environment, these systems can encounter unexpected relocation of services. • Idle time is reset on broadcast message when AdvFS is the root file system. • Fixes an AdvFS hang that could occur while running vdump. • AdvFS hangs in routine cleanup_closed_list. • A panic that is seen when running the auditd and auditing msfs_syscall. There will most likely be a lot of memory contention as well for this panic to be triggered. • NFS rpc.lockd "can't clear lock after crash of client" when AdvFS is being used. • A system may hang when an application or program attempts to read a file on an AdvFS system. • Fixes a system panic with the message "simple_lock: time limit exceeded". • Fixes an "ADVFS EXCEPTION, Module = 26" panic that occurs after an "advfs I/O error" console message. • Fixes a problem that occurs on AdvFS systems. When a user exceeds the quota limits, an excessive number of user warning messages are sent to the system console if the user terminal is inaccessible.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 503.01 continued	• Fixes an AdvFS problem that causes the system to panic with the following error message: simple_lock: lock already owned by cpu • Fixes a system panic when shutting down to single user mode using one of the following commands: – # shutdown now – # init s when AdvFS is the root or usr filesystem. • Fixes a problem where the vrestore program does not report failed exit status appropriately on incomplete or incorrect commands, corrupt or invalid saved sets, or file open failures. • Fixes a problem that occurs on SMP systems with an AdvFS filesystem in which the system panics with the following message: simple_lock: time limit exceeded • Fixes a problem that occurs on systems running AdvFS. The system panics with the following error message: panic (cpu 0): bfs_invalidate: not on free list syncing disks...done • When a user attempted to restore a vdump, which had been done with the "-D" option and included directories for which Access Control Lists (ACL's) had been declared, the vrestore program was failing to restore ACL's on directory files and issued warning messages. When a user specified the "-t" option, vrestore erroneously attempted to restore proplists on files that had them; issuing warning messages. • Fixes a problem that occurs on AdvFS systems. The system will panic with an error message similar to the following: panic (cpu 0): kernel memory fault • Corrects problems with AdvFS performance regression, and two AdvFS race condition situations between multiple routines that can cause panics. • Fixes a problem that occurs on an AdvFS file system. The system may panic with the following error message: ADVFS INTERNAL ERROR: dealloc_bits_page: can't clear a bit twice • Fixes two problems that occur on AdvFS systems: – The system may panic with the following error message: simple_lock: hierarchy violation – A locking problem in the AdvFS log data structures may cause the following problems to occur: ☐ System panics ☐ Kernel memory faults ☐ Memory corruption

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 503.01 continued	• Fixes a problem that occurs on AdvFS systems. If the "ls -l M1" command is given in a .tags directory, the fileset will become unmountable. If the system is then halted, a panic will occur. • Fixes an AdvFS problem in which improper handling of I/O queues cause either a kernel memory fault or the following panics: "bs_invalidate: cache rundown" "rm_or_moveq: ioDesc not on a queue" • Corrects a problem in AdvFS where a data structure field is not initialized until after an AdvFS mount which is too late. This results in the inability for example to see the files after a remount. • Fixes a problem that occurs on an AdvFS file system. While the symptoms of these AdvFS problems vary, the most common is a panic with the following error message: bs_frag_alloc: pinpg faild\n N1 = -1035 Alternately, bs_frag_dealloc: pinpg faild\n N1 = -1035 • Fixes an AdvFS problem in which improper handling of I/O queues cause either a kernel memory fault or the following panics: "bs_invalidate: cache rundown" "rm_or_moveq: ioDesc not on a queue" • Corrects a problem in AdvFS where a data structure field is not initialized until after an AdvFS mount which is too late. This results in the inability for example to see the files after a remount. • Fixes a problem that occurs on an AdvFS file system. While the symptoms of these AdvFS problems vary, the most common is a panic with the following error message: bs_frag_alloc: pinpg faild\n N1 = -1035 Alternately, bs_frag_dealloc: pinpg faild\n N1 = -1035
Patch 508.00 OSF400CDE-006B	**Patch:** OSF400CDE-006B **State:** New patch This patch fixes a problem in which users logging into a system that has a nodename longer than 32 characters cause ttsession to core dump. This only happens when using CDE desktop.
Patch 509.00 OSF400-410D	**Patch:** Math Library Function Corrections **State:** New patch • Fixes the problem of the math library functions not returning the correct NaN value as defined in the Alpha AXP Architecture Reference Manual (Second Edition). • Fixes a problem with fastmath functions F_Exp() and F_Pow() that would cause floating exception core dumps.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 510.00 OSF400-203B	**Patch:** auth_for_terminal() Segmentation Fault Correction **State:** New patch This patch corrects the following: • Under enhanced security, sometimes users (even root) are unable to log in on graphics console, even after using dxdevices or edauth to clear the t_failures count. • On systems running enhanced security, user-written applications that call auth_for_terminal() may fail with a segmentation fault.
Patch 511.00 OSF400-364B	**Patch:** System Run Level Correction **State:** New patch This patch fixes two system run level problems: • On a system running LSM, whenever there is a run level change, the lsmbstartup script runs. This causes root to be mounted read/write in single-user mode. • The bcheckrc command script continues to run even if there is an invalid root entry. This leaves the system in an unusable state in single-user mode.
Patch 512.00 OSF400-371B	**Patch:** uprofile And Kprofile Command Corrections **State:** New patch This patch fixes the following problems: • The uprofile and kprofile commands report incorrect statistics on an SMP system or when trying to measure EV5 events other than cycles. • The pfm driver ioctl PCNT5GETCNT returns incorrect data. • An unstoppable stream of pfm interrupts is produced if an EV5 machine is rebooted with the pfm driver active. • The pfm(8), uprofile(1), and kprofile(1) manpages do not describe the EV5 statistics supported by the software.
Patch 513.00 OSF400-487B	**Patch:** Run-Time Support For DIGITAL C++ V6.0 Compiler **State:** New patch This patch provides the requried run-time support for images created by the DIGITAL C++ V6.0 and above compiler. Contact the DIGITAL C++ compiler group (cxx@lego.zko.dec.com) for details.
Patch 514.00 OSF400CDE-013B	**Patch:** Security, (SSRT0498U) **State:** New patch A potential security vulnerability has been discovered in 'libDtSvc', where under certain circumstances users may gain unauthorized access. DIGITAL has corrected this potential vulnerability.

Table 6–2: Summary of patches in Patch Kit-0006 (cont.)

Patch 515.00 OSF400-405B	**Patch:** Greater Than 500 XTI Connections Crash Correction **State:** New patch This patch corrects the following: • Fixes the problem of t_optmgmt() T_NEGOTIATE calls returning T_SUCCESS, but not actually negotiating the socket options. This behavior is a UNIX95 specification standard compliance bug. • Fix for a problem that manifests itself by the system hanging or becoming inoperable when a number of XTI connections reaches 500. • Resolves a hang in the xticlose() routine and a kernel memory fault in the xti_discon_req() routine. • Corrects a problem with the xti/streams interface module which could result in a kernel memory fault panic during use by xti application programs. • Fixes a problem with the implementation of the TPI interface. This problem occurs if you are using DIGITAL's XTI libxti library with a third-party (non-DIGITAL) STREAMS driver.

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
```