Oracle® Solaris 11.3 Security Compliance Guide

Part No: E54817
March 2018

ORACLE

Oracle Solaris 11.3 Security Compliance Guide

Part No: E54817

Référence: E54817

Accès aux services de support Oracle

Les clients Oracle qui ont souscrit un contrat de support ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` ou le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` si vous êtes malentendant.

Contents

Using This Documentation

- **Overview** – Describes how to assess and report the compliance of Oracle Solaris systems to security benchmarks and customized tailorings of benchmarks. Also describes how to verify that a system has installed the latest Oracle Critical Patch Updates that repair Common Exposures and Vulnerabilities (CVE).
- **Audience** – Security administrators and auditors who assess security on Oracle Solaris 11 systems.
- **Required knowledge** – Site security requirements.

Product Documentation Library

Documentation and resources for this product and related products are available at http://www.oracle.com/pls/topic/lookup?ctx=E53394-01.

Feedback

Provide feedback about this documentation at http://www.oracle.com/goto/docfeedback.

♦ ♦ ♦ CHAPTER 1

Reporting Compliance to Security Standards

This chapter describes how to assess and report the compliance of an Oracle Solaris system to security standards, also called *security benchmarks* and *security policies*. It also describes how to create an adjunct to a benchmark, called a tailoring, to evaluate the compliance of systems with specialized policy. This chapter covers the following topics:

What's New in Compliance in Oracle Solaris 11.3

This section highlights information for existing customers about important new compliance features in this release.

- Compliance rules that are coded with variable values enable you to create tailorings whose rules check for the precise values that satisfy site security requirements. See "Selecting Alternate Values for Variables in Compliance Rules" on page 29 and the `compliance-tailor`(1M) man page.
- You can schedule compliance assessments to run periodically. This functionality is disabled by default. See "Running Assessments at Regular Intervals" on page 31 and the `compliance`(1M) man page.

About Compliance in Oracle Solaris

Systems that comply with security standards provide more secure computing environments, and are easier to test, maintain, and protect. Oracle Solaris provides scripts that assess and report the compliance of your Oracle Solaris system to two security benchmarks: Solaris Security Benchmark and Payment Card Industry-Data Security Standard (PCI DSS).

Compliance assessment is critical for validating system compliance to external and internal security policies. The handling of security compliance and auditing requirements accounts for a large percent of IT security spending, including documentation and reports, and the validation itself. Organizations such as banks, hospitals, and governments have specialized compliance requirements. Auditors who are unfamiliar with an operating system can struggle to match security controls with requirements. Therefore, tools that map security controls to requirements can reduce time and costs by assisting auditors.

Compliance assessment is based on scripts. The scripts follow the Security Content Automation Protocol (SCAP), written in Open Vulnerability and Assessment Language (OVAL). The SCAP implementation in Oracle Solaris also supports scripts that conform to the Script Check Engine (SCE). These scripts add security checks that the current OVAL schemas and probes do not provide.

For information about the SCAP set of tools that support the `compliance` command, see the `oscap`(8) man page. To display the version of the SCAP set of tools, issue the `oscap -V` command.

Note - The SCAP set of tools cannot localize the reports that the `oscap` command produces, nor can it localize the test descriptions.

Additional scripts can be used to meet other regulatory environment standards, such as the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes Oxley (SOX), and the Federal Information Security Management Act (FISMA). For links to these standards, see Appendix A, “Compliance Reference”.

Security Benchmarks and Oracle Solaris

Oracle Solaris supplies compliance scripts for two standards: Solaris and PCI DSS. Independently, Center for Internet Security (CIS) provides a third-party benchmark for Oracle Solaris. You can also create customized assessments based on security benchmarks and profiles, called tailorings.

Solaris Security Policy Benchmark

The Solaris security policy benchmark is a standard based on the "secure by default" (SBD) default installation of Oracle Solaris.

The benchmark provides two profiles: `Baseline` and `Recommended`.

- The `Baseline` profile of the Solaris benchmark closely matches the default SBD installation of Oracle Solaris.
- The `Recommended` profile satisfies organizations with stricter security requirements than the `Baseline` profile. Systems that comply with the `Recommended` profile also comply with the `Baseline` profile.

The features which comprise SBD are described in "Using the Secure by Default Configuration" in *Securing Systems and Attached Devices in Oracle Solaris 11.3* and "Oracle Solaris Configurable Security" in *Oracle Solaris 11.3 Security and Hardening Guidelines*.

The Solaris benchmark does not satisfy the requirements of the PCI DSS, CIS, or Defense Information Systems Agency-Security Technical Information Guides (DISA-STIG) benchmarks for Oracle Solaris.

PCI DSS Security Policy Benchmark

The PCI DSS security policy benchmark is a proprietary information security standard for organizations that handle cardholder information for major debit and credit cards. The standard is defined by the Payment Card Industry Security Standards Council. The intent is to reduce credit card fraud.

An Oracle Solaris system requires configuration to comply with the PCI DSS standard. The compliance report indicates which tests failed and which tests passed, and provides remediation steps. Because some PCI DSS requirements do not correspond directly to software, you must examine the compliance report and then perform additional tasks to comply with the standard. For more information, see *Meeting PCI DSS Compliance with Oracle Solaris 11*.

CIS Benchmark for Oracle Solaris

The CIS standards organization provides automated compliance checking tools for its Oracle Solaris benchmark. Contact CIS to determine the cost of using CIS tools. You can use them on a Microsoft Windows system for checking Oracle Solaris compliance.

Tailorings From Benchmarks

You can create *tailorings* from security policy benchmarks. Tailorings customize assessments to verify the security policy of particular systems at your site. To create these customized assessments, you include or exclude rules from an existing benchmark, profile, or tailoring. To use a tailoring to assess systems, you must install the source benchmark as well as the tailoring. For more information, see "Security Benchmarks and Oracle Solaris" on page 10 and "Creating Tailorings From Compliance Benchmarks" on page 18.

compliance Command and Package

To measure security compliance, hereafter called *compliance*, requires a set of rules that define a security benchmark or profile; a measurement of compliance to that benchmark, called an *assessment*; and then a report of the findings. The report can also be printed in guide form for training or archiving purposes.

Oracle Solaris provides the `compliance` command to measure security security compliance. The command can generate, list, and delete assessments and reports. While any user can view compliance reports, you must have rights to manage and generate assessments. For more information, see "Rights to Run the compliance Command" on page 12 and the `compliance`(1M) man page.

The `compliance` command checks local files only. If your system mounts file systems, you must separately test the compliance of the clients and the servers. For example, if you mount user home directories from central servers, run the command on the user systems and on every home directory server.

Note - The `compliance` command automates compliance assessment, not remediation.

Rights to Run the compliance Command

Oracle Solaris provides two rights profiles to handle compliance assessment and report generation.

- The Compliance Assessor rights profile enables users to perform assessments, place them in the assessment store in report format, and delete assessments from the store.

- The Compliance Reporter rights profile enables users to locate and display existing assessments.

Compliance subcommands require the following rights:

- `compliance assess` command – Requires all privileges and the `solaris.compliance.assess` authorization. The Compliance Assessor rights profile provides these rights.
- `compliance delete` command – Requires write access to the assessment store and the `solaris.compliance.assess` authorization. The Compliance Assessor rights profile provides these rights.
- `compliance list` command – Can be run by anyone who has basic rights. This command provides full visibility to both benchmarks and assessments.
- `compliance report` command – Can be run by anyone, but the range of functionality varies according the user's rights. Users who are assigned either the Compliance Assessor or Compliance Reporter profile can generate new reports in the assessment store. All users can view existing reports, but users with only basic rights cannot generate reports.
- `compliance tailor` command – Can be run by users who are assigned the Compliance Assessor profile.

`compliance` Package

The compliance rules, benchmarks, profiles, and commands are available in the `pkg:/security/compliance` package. The `solaris-small-server` and `solaris-large-server` package groups install this package.

- For information about package groups, see "Installing the Oracle Solaris OS" in *Oracle Solaris 11.3 Security and Hardening Guidelines*.
- For information about packages, see *Oracle Solaris 11.3 Package Group Lists*.
- For a description of the compliance package, issue the `pkg info compliance` command.

Compliance Reports and Guides

Oracle Solaris provides three formats for compliance reports and a guide for each benchmark and profile.

Assessment Report Formats

After you have run an assessment, the assessment directory contains a log file, a report, and a guide of your system's compliance to that specific assessment. The assessment directory files contain the following information:

- `log` – In text form, contains the results for every test that was performed for the assessment and its rule ID. The following example shows a sample entry:

```
Title   The OS version is current
Rule    OSC-53005
Result  pass
```

- `report.html` – In browser-ready form, contains the results for every test that was performed for the assessment and its rule ID, time the test was run, compliance severity (high, medium, or low), description, and remediation assistance. The following example shows a sample entry:

```
    Result for Package integrity is verified
    Result: fail
    Rule ID: OSC-54005
    Time: 2014-09-03
      13:35
    Severity: high
      Run 'pkg verify' to check that all installed Oracle Solaris software matches
      the packaging database and that ownership, permissions and content are correct.

     Remediation instructions
      'pkg verify' has produced errors. Rerun the command and evaluate the errors.
       As appropriate, based on errors found,you should run 'pkg fix <package-fmri>'
       See the pkg(1) man page.

    Remediation script
    # pkg verify
    followed by
    # pkg fix <package-fmri>

The following packages showed errors
    pkg://solaris/library/perl-5/sun-solaris-512          ERROR
```

- `results.xccdf.xml` – Contains the results of every test in the benchmark. In addition to the information that is covered in `report.html`, the guide contains introductions to the areas that are assessed and references to Oracle Solaris system administration guides.

Oracle Solaris Compliance Guides

At installation, the `compliance` package provides guides to the compliance benchmarks and profiles. A guide contains the rationale for each security check and the steps to fix a failed check. Guides can be useful for training and as guidelines for future testing.

The guides that are installed with the `compliance` package are:

- *benchmark* guide – Contains every test in *benchmark*. Examples are `pci-dss`, `solaris_pci-dss`, and `solaris`.
- *benchmark.profile* guide – Contains every test in *benchmark*, plus a table at the end of the guide that lists which tests are selected or not selected for *profile*. Examples are `solaris.baseline` and `solaris.recommended`.

New Guides for New Benchmarks

The `compliance:generate-guide` service creates guides for each security benchmark and profile at installation. If you add a new benchmark or profile, you can create a guide for it.

```
# compliance guide -a
```

Administering Compliance Assessments and Reports

Compliance assessments of a benchmark or profile are comprehensive. They check every rule. Reports can include every rule or a subset of the rules in the assessment. You can run assessments regularly by using the scheduled method of the `compliance:default` service. For more information, see “Running Assessments at Regular Intervals” on page 31.

Listing Compliance Information and Locating Assessments and Reports

The `compliance list` command is available to all users. With the verbose `-v` and profile `-p` options, this command lists the benchmarks and their short descriptions; the profiles for each benchmark; assessments and whether reports exist for them; and reports.

EXAMPLE 1 Listing All Benchmarks, Profiles, Assessments, and Reports

In this example, the administrator has specified `pci` and `recommended` on the command line as assessment names. The other assessment names were generated by the `compliance assess` command without specified assessment names.

```
$ compliance list -vp
Benchmarks:
pci-dss:        Solaris_PCI-DSS
                PCI-DSS Security/Compliance benchmark for Oracle Solaris
solaris:        Baseline, Recommended
                Oracle Solaris Security Policy
Assessments:
pci:    log report.html results.xccdf.xml
recommended:   log report.html report.xml results.xccdf.xml results.xml
pci-dss.Solaris_PCI-DSS.2015-10-10,10:12:       log report.html results.xccdf.xml
solaris.Baseline.2015-10-10,15:10:      log report.html results.xccdf.xml
solaris.Baseline.2015-10-10,15:20:      No reports have been generated
```

EXAMPLE 2 Locating Files in the Compliance Repository

The reports of assessments are stored in the `/var/share/compliance/assessments` directory, also known as the repository. In this example, an administrator with the Compliance Reporter rights profile views the names and locations of the reports in the `recommended` directory.

```
$ pfexec compliance report -a recommended
/var/share/compliance/assessments/recommended/report.html

$ compliance report -f log -a recommended
/var/share/compliance/assessments/recommended/log

$ compliance report -f xccdf -a recommended
/var/share/compliance/assessments/recommended/results.xccdf.xml
```

Running Assessments and Reports

The `compliance` package is required to run assessments and reports. By default, the `solaris-small-server` and `solaris-large-server` packages include the `compliance` package. The `solaris-desktop` and `solaris-minimal` packages do not include the `compliance` package. To manage the assessment directories and reports in the repository requires privilege.

You can create assessment reports for benchmarks, profiles, and tailorings. For information about tailorings, see “Creating Tailorings From Compliance Benchmarks” on page 18.

You can run a specified assessment on a system at regular intervals, as described in "Running Assessments at Regular Intervals" on page 31.

▼ How to Run Assessments and Reports

In this procedure, you create assessment reports locally.

Before You Begin You must be assigned the Software Installation rights profile to add packages to the system. You must be assigned administrative rights for most compliance commands, as described in "Rights to Run the `compliance` Command" on page 12. For more information, see "Using Your Assigned Administrative Rights" in *Securing Users and Processes in Oracle Solaris 11.3*.

1. Install the `compliance` package in every zone where you plan to run compliance tests.

```
$ pkg install compliance
```

The following message indicates that the package is installed:

```
No updates necessary for this image.
```

For more information, see the `pkg`(1) man page.

2. List the benchmarks and profiles that are available.

```
$ compliance list -p
Benchmarks:
pci-dss:        Solaris_PCI-DSS
solaris:        Baseline, Recommended
Assessments:
      No assessments available
```

3. Create an assessment.

```
$ pfexec compliance assess -p profile -b benchmark -a assessment-name
```

-p *profile*	Indicates the name of the profile. The profile name is case sensitive.
-b *benchmark*	Indicates the name of the benchmark. The benchmark name is case sensitive.
-a *assessment-name*	Optional. Indicates the name of the assessment. The default name includes a time stamp.

For example, the following command assesses the system using the `Recommended` profile and creates an assessment directory in the compliance repository for the assessment named `recommended`.

```
$ pfexec compliance assess -p Recommended -b solaris -a recommended
```

After the command completes, the reports are stored in a plain text log file named `log`, an XML file named `results.xccdf.xml`, and an HTML file named `report.html`.

```
$ pfexec compliance list -v -a recommended
recommended:      log report.html results.xccdf.xml
```

If you run the same `compliance assess` command again, the files are not replaced. Supply a different name for the directory or do not use the `-a` option.

4. **View the full report.**
   You can view the log file in a text editor, view the HTML file in a browser, or view the XML file in an XML viewer.
   For example, to view `report.html`, type the following browser entry:

   ```
   file:///var/share/compliance/assessments/recommended/report.html
   ```

5. **Fix any failures that must pass.**

   a. **Complete the fix for the entry that failed.**

   b. **If the fix includes rebooting the system, reboot the system before running the assessment again.**

Creating Tailorings From Compliance Benchmarks

The benchmarks that Oracle Solaris provides might report failures or false positives that do not accurately reflect the compliance of particular systems. For these systems, you can create *tailorings*, which are inclusions or exclusions of rules, or modifications of rules with variable values, from these benchmarks. Rules with variable values are explicitly marked in the interface. By modifying a variable used in a rule, you can include the rule while providing a more fine-grained expression of your security policy. You can then use these tailorings to assess the security posture of your site.

You create a tailoring by including or excluding rules from a benchmark, profile, or tailoring, then saving the new rule set under a different name. You can create multiple tailorings from a

source benchmark and the tailorings are independent of each other. Every tailoring has a unique name.

You can use tailorings to assess the compliance of systems to a few rules or to many rules. You can save a tailoring in a form to be incorporated in an IPS package for installation on many systems. See "How to Create a Package Manifest for a Tailoring" on page 25.

Users who are assigned the Compliance Assessor rights profile can create tailorings and run assessments and reports. For details, see "Rights to Run the `compliance` Command" on page 12. To create a tailoring, you modify the selection of rules in a benchmark or profile. You do not and cannot modify the rules themselves. Because the source of a tailoring is a particular benchmark, that benchmark must be installed on a system where you run the tailoring.

Tip - Before creating a tailoring, print the table of contents for your source benchmark or profile. The table of contents contains the titles and numbers of the rules that you might want to exclude or include in your tailoring. Good sources for a table of contents are the guide for a benchmark or a compliance report in HTML format.

- If the tailoring will modify only a few rules from the source, start the tailoring by excluding all rules (`exclude -a`), then include the few rules you want or change the variable values of certain rules.
- Otherwise, exclude or include a few rules from the source benchmark or profile, or change the variable values of certain rules.

Editing Compliance Tailorings

The `compliance tailor` command provides two editing options, an interactive command-line editor and a curses editor, called the *pick screen*.

The pick screen is implemented in the curses programming language. It provides GUI-like functionality on a text-only device, such as a console or a hardware ANSI terminal.

▼ How to Create a Tailoring From a Compliance Benchmark

Before You Begin

You must be assigned the Compliance Assessor rights profile to create a tailoring that can be added to the system store. For more information, see "Rights to Run the `compliance`

Command" on page 12 and "Using Your Assigned Administrative Rights" in *Securing Users and Processes in Oracle Solaris 11.3*.

1. **Open the compliance editor.**

   The following command sets options on the command line and opens the pick screen.

   ```
   $ pfexec compliance tailor -t basic
   *** compliance tailor: Can't get existing tailor "basic", initializing
   tailoring:basic> set benchmark=solaris
   tailoring:basic> exclude -a
   tailoring:basic> pick
   ```

   where

   - `basic` is the name of the tailoring
   - `solaris` is the source benchmark
   - `exclude -a` loads the `solaris` benchmark with none of the rules included
   - `pick` opens the pick screen

   The pick screen displays all of the rules in the `solaris` benchmark. None of them are included.

2. **On the pick screen, use the keyboard to include particular rules, exclude rules, and navigate.**

   - The spacebar toggles between including and excluding an entry.
   - An `x` indicates an excluded rule.
   - A greater-than symbol (>) in reverse video indicates an included rule. No `x` is a second indication that the rule is included.
   - An `exit` or ESC returns you to the `compliance tailor` command line in interactive mode.

3. **Include a few basic rules.**

   For example, you might include the rules OSC-53005, OSC-16005, OSC-35000, OSC-46014, OSC-01511, OSC-04511, and OSC-75511.

4. **Commit your changes then exit the command-line interface.**

   ```
   tailoring:basic> commit
   tailoring:basic> exit
   $
   ```

   Tailorings that you create with the `compliance tailor` declare the benchmark and profile inside them.

5. **(Optional) Verify that the tailoring is in stable storage.**

```
$ pfexec compliance tailor list
basic
```

6. **Test the tailoring and evaluate the output.**

```
$ pfexec compliance assess -t basic
Assessment will be named 'basic.2015-10-10,10:10'
Title   The OS version is correct
Rule    OSC-53005
Result  pass
...
Title   Stacks are non-executable
Rule    OSC-75511
Result  pass
```

7. **(Optional) Display the assessment report in a browser.**

   a. **Locate the assessment.**

```
# compliance report
/var/share/compliance/assessments/basic.2015-10-10,10:10/report.html
```

   b. **Load the assessment into the browser.**

   The following example shows a sample browser entry:

```
file:///var/share/compliance/assessments/basic.2015-10-10,10:10/report.html
```

Example 3 Loading a Different Tailoring

In this example, the administrator loads tailorings that are stored but not in current use.

```
$ pfexec compliance tailor
tailoring>list
basic
firsttest
testg
tailoring>load firsttest
tailoring:firsttest>info
    tailoring=firsttest
    benchmark=solaris
    profile: not set
tailoring:firsttest>load testg
tailoring:testg>
```

How to Update Tailorings Based on Previous Benchmark Versions

You can discover that you have an outdated tailoring after updating Oracle Solaris. This procedure shows how to update or delete the tailoring.

Before You Begin You must be assigned the Compliance Assessor rights profile.

1. **Run an assessment by using the tailoring.**

```
$ pfexec compliance assess -t tailoring
WARNING: version mismatch between tailoring 'tailoring'(1.nnnn) and
benchmark 'solaris'(1.higher-nnnn), assessment test selections may not be as expected
```

2. **Review the report.**
   If the results are what you expect, then you can update the tailoring to the current benchmark or profile version. If the results do not accurately report the compliance of the system, you can modify the tailoring or create a new one.

3. **View the contents of the tailoring.**

```
$ pfexec compliance tailor -t tailoring
*** compliance tailor: WARNING: version mismatch between tailoring 'tailoring'(1.nnnn)
 and
benchmark 'solaris'(1.higher-nnnn), assessment test selections may not be as expected
tailoring:basic> export
...
```

4. **(Optional) To delete the tailoring, type `delete` in the interactive interface and confirm the deletion.**

```
tailoring:basic> delete
OK to delete tailoring 'basic' (y/N)? y
$
```

5. **If needed, modify the tailoring to create the correct assessment.**

```
tailoring:basic> exclude OSC-nnnnn
tailoring:basic> include OSC-nnnnn
...
tailoring:basic> export
tailoring:basic> commit
tailoring:basic> exit
```

   For a different update method, see Example 4, “Updating a Tailoring From an Export File,” on page 23.

6. **Verify that your assessment runs without error.**

```
$ pfexec compliance assess -t tailoring
Assessment will be named 'tailoring.YYYY-MM-DD,HH:MM
```

Example 4 Updating a Tailoring From an Export File

The administrator imports the outdated tailoring to verify that its output is accurate.

1. Using the `pfexec compliance tailor` command, the administrator opens the tailoring and exports it to a file.

```
$ pfexec compliance tailor -t myTailoring
*** compliance tailor: WARNING: version mismatch between tailoring
 'myTailoring'(1.1234) and
benchmark 'solaris'(1.2345), assessment test selections may not be as expected
tailoring:myTailoring> export -o myTailoring1.txt
tailoring:myTailoring> exit
```

2. The administrator edits the export file to rename the tailoring.

```
$ pfedit myTailoring1.txt
set tailoring=myTailoring1
```

3. The administrator imports the modified exported rule set.

```
$ pfexec compliance tailor -f myTailoring1.txt
tailoring:myTailoring1> commit
tailoring:myTailoring1> exit
```

4. The administrator verifies that the new tailoring performs the same job as the original tailoring.

```
$ pfexec compliance assess -t myTailoring1
...
```

5. The administrator deletes the outdated tailoring.

```
$ pfexec compliance tailor -t myTailoring
tailoring:myTailoring> delete
OK to delete tailoring 'myTailoring' (y/N)? y
$
```

Troubleshooting If you are denied permission to update or delete the tailoring, either assume the `root` role, or if you have the Compliance Assessor rights profile, precede the `compliance tailor` command with `pfexec`.

How to Export a Tailoring

Exporting a tailoring lets you examine it for completeness. The export file contains comments that describe the rules that are included and excluded. You can use this file to import the tailoring on a different system for further testing. The directory to which you export the tailoring must be writable by you.

You can also use the `export` command to create a file for an IPS package of your tailoring. See "How to Create a Package Manifest for a Tailoring" on page 25.

1. **Load and export the tailoring.**

   The `-o` option specifies the file name. In this example, the administrator uses the `txt` file extension to indicate that the file is in plain text.

```
$ pfexec compliance tailor
tailoring>list
basic
testg
tailoring>load basic
tailoring:basic> export -o /home/jdoe/basic.tailor.txt
```

2. **When the new tailoring is ready for production, export it in XML format by using the `-x` option.**

   In this example, the administrator uses the `xccdf.xml` file extension to indicate that the file is in the required format for an IPS package.

```
$ pfexec compliance tailor -t basic
tailoring:basic> export -x -o /home/jdoe/basic.xccdf.xml
tailoring:basic> exit
```

Example 5 Creating a Kerberos Tailoring From the `Recommended` Profile

In this example, the administrator creates a tailoring that includes Kerberos compliance rules. The administrator sets the source benchmark and profile and creates a tailoring from the profile plus rules that apply to Kerberos. The `export` command shows the effects of the rule inclusions and exclusions.

```
$ pfexec compliance tailor -t RKerberos
tailoring:RKerberos>set benchmark=solaris
tailoring:RKerberos>set profile=Recommended
tailoring:RKerberos>exclude OSC-28010
tailoring:RKerberos>exclude OSC-30510
tailoring:RKerberos>exclude OSC-31010
tailoring:RKerberos>exclude OSC-31510
```

```
tailoring:RKerberos>exclude OSC-63005
tailoring:RKerberos>include OSC-02511
tailoring:RKerberos>commit
tailoring:RKerberos>export
set tailoring=RKerberos
# version=2015-10-10T20:20:20.000+00:00
set benchmark=solaris
set profile=Recommended
# OSC-28010: Service svc:/network/security/kadmin is disabled or not installed
exclude OSC-28010
# OSC-30510: Service svc:/network/security/krb5_prop is disabled or not installed
exclude OSC-30510
# OSC-31010: Service svc:/network/security/krb5kdc is disabled or not installed
exclude OSC-31010
# OSC-31510: Service svc:/network/shell:kshell is disabled or not installed
exclude OSC-31510
# OSC-62511: Service svc:/network/rpc/gss is enabled
include OSC-62511
# OSC-63005: Service svc:/network/rpc/gss is enabled if and only if Kerberos is
 configured
exclude OSC-63005
```

▼ How to Create a Package Manifest for a Tailoring

After testing your new tailoring thoroughly, you can create an IPS package to install the new rules file. The *package manifest* is an early step in package creation. For the steps in creating a package, see *Packaging and Delivering Software With the Image Packaging System in Oracle Solaris 11.3*.

1. **Export a thoroughly tested tailoring.**

```
$ pfexec compliance tailor -t basic
tailoring:basic> export -x -o basic.xccdf.xml
tailoring:basic> exit
```

The package that you create installs this file.

2. **Create a manifest with the package name and the suffix `.p5m`.**

Tip - Create your manifest in a working directory that will not be overwritten during updates, such as your home directory.

The following output shows a sample template for a package manifest for a tailoring. This tailoring is based on the `solaris` benchmark, so the tailoring package is dependent on the

`solaris-policy` package, which installs the `solaris` benchmark. The items in bold in the manifest are invariant. Long lines are continued on an indented second line for ease of reading. In the manifest, the lines are not broken.

```
$ pfedit solaris-basic.p5m
set name=pkg.fmri value=pkg://publisher-name/hierarchical-namepkg-name@mainVersion.revision
set name=pkg.summary value="summary"
set name=pkg.description value="description"
file ./exported-rules-file group=group mode=permissions owner=owner
    path=usr/lib/compliance/benchmarks/solaris/tailorings/installed-rules-file.xml
depend fmri=pkg:/security/compliance/benchmark/solaris-policy type=require
```

where

- `pkg.fmri value=` specifies the full name of the package. You provide this name. The publisher name is optional. You can provide it here or when you publish the package.
- `pkg.summary value=` specifies the information that displays in the Summary field of the `pkg info` *mainVersion* command. You write the summary.
- `pkg.description value=` specifies the information that displays in the Description field of the `pkg info` *mainVersion* command. You write the description.
- `file` specifies where the tailoring is installed. The specification includes the source name and the installed name of the rules file for the tailoring, the directory location of the installed file without the initial slash (`usr/lib/compliance/benchmarks/solaris/tailorings`), and DAC permissions. The DAC permissions and location are fixed. You provide the name of the rules file that the package installs on the system. The name of the source rules file can be different from its installed version.
- `depend` specifies that the package that delivers the source benchmark for your tailoring will be installed on your system if it is not already installed. This entry is required.

  Because `basic` tailoring is based on the `solaris` benchmark, the `solaris-policy` package will be installed on your system if it is not already installed. The `solaris-policy` package installs the directory `/usr/lib/compliance/benchmarks/solaris/tailorings` where your tailoring file is placed. To view the specification of this package, type the `pkg contents -m solaris-policy` command.

Caution - In your package manifest, do not duplicate a path that has already been specified by a package that your package depends on.

3. Create a manifest file from an existing file.

a. Use the following example text as your manifest file.

In this sample manifest, the `solaris-basic.exportx.xml` file from the `example-IT` repository is installed as the file `basic.xccdf.xml`.

```
set name=pkg.fmri value=pkg://example-IT/security/compliance/tailorings/solaris-
basic@1.0
set name=pkg.summary value="Tailors a basic Solaris compliance assessment for all
    systems"
set name=pkg.description value="This Solaris basic tailoring is applicable to all
    systems, development and production. All Oracle Solaris systems are expected
    to pass the rules in this tailoring."
file ./solaris-basic.exportx.xml group=sys mode=0555 owner=root
    path=usr/lib/compliance/benchmarks/solaris/tailorings/basic.xccdf.xml
depend fmri=pkg:/security/compliance/benchmark/solaris-policy type=require
```

b. Modify the file, then save it.

Note - Be careful when typing the content of a package manifest. Make sure you join the lines that were too long to display on a single line.

Example 6 Creating a Package Manifest for a Compliance Package for Oracle Solaris NFS Clients

This example shows how to create a package manifest for a tailoring for NFS clients. The source name of the rules selection file is `solaris-Baseline-nfs-client.exportx.xml`. Its installed version is `nfs-client.xccdf.xml`. The tailoring is based on the `Baseline` profile of the `solaris` benchmark, so the package is dependent on the `solaris-policy` package.

1. Export the tailoring and quit the editor.

```
$ pfexec compliance tailor -t solaris-Baseline-nfs-client
tailoring:solaris-Baseline-nfs-client> export -x -o sB-nfs-client.exportx.xml
tailoring:solaris-Baseline-nfs-client> exit
```

2. Create a manifest with the package name and fill out the manifest.

```
$ pfedit /home/ooyl/packages/tailorings/solaris-Baseline-nfs-client.p5m

set name=pkg.fmri value=pkg://corporate-IT/security/compliance/tailorings/
    solaris-Baseline-nfs-client@1.0
set name=pkg.summary value="An NFS client tailoring for Solaris Baseline systems."
set name=pkg.description value="This NFS tailoring is an adjunct to the solaris.
Baseline
    profile. Assess all NFS client systems with this nfs-client tailoring."
file ./sB-nfs-client.exportx.xml group=sys mode=0555 owner=root
    path=usr/lib/compliance/benchmarks/solaris/tailorings/nfs-client.xccdf.xml
depend fmri=pkg:/security/compliance/benchmark/solaris-policy type=require
```

Note - A tailoring that is installed as a package is stored in the `/usr/lib/compliance/benchmarks/`*name*`/tailorings` directory.

Example 7 Creating Assessments and Reports From Tailorings

In this example, an administrator has installed two tailoring packages and has a tailoring testing file. `solaris/` indicates that the installed tailoring packages are based on the `solaris` benchmark.

```
$ compliance tailor list
solaris/basic
solaris/RKerberos
testBaselinePlus
```

The Compliance Assessor administrator runs the installed tailorings assessments and views the results in a browser.

1. The administrator runs assessments for both tailorings.

```
$ pfexec compliance assess -t solaris/basic
Assessment will be named "basic.2015-11-12,10:10"
Title   The OS version is correct
Rule    OSC-53005
Result  pass
...
% compliance report
/var/compliance/assessments/solaris/basic/basic.2015-11-12,10:10/report.html

$ pfexec compliance assess -t solaris/RKerberos
Assessment will be named "RKerberos.2015-11-12,10:20"
...
Title   Service svc:/network/rpc/gss is enabled
Rule    OSC-62511
Result  pass
...
$ compliance report
/var/compliance/assessments/solaris/RKerberos/RKerberos.2015-11-12,11:10/report.html
```

2. The administrator views the reports by typing the following entries in a browser.

```
file:///var/share/compliance/assessments/solaris/basic/basic.2015-11-12,10:10/report.
html
```

```
file:///var/share/compliance/assessments/solaris/RKerberos/RKerberos.2015-11-12,11:
10/report.html
```

Next Steps To complete the testing and delivery of this package, see *Packaging and Delivering Software With the Image Packaging System in Oracle Solaris 11.3*. You should sign your tailoring packages. The packaging utility includes other attributes, such as facets, that you might want to use in the package manifest.

Selecting Alternate Values for Variables in Compliance Rules

Selecting an alternate value for a compliance rule value is called *value tailoring*. Value tailoring enables you to more finely tune your tailoring. Instead of removing a rule that does not reflect your site security requirements, you can set the rule's variable value to a value that reflects site policy. For example, you might modify the rule for password length to check for a password length of `13` characters rather than `8`, or for a service that is enabled rather than disabled as in the default configuration.

Note - You can modify the value of a rule only if that value is declared as a variable. Not all rules are coded with variable values.

You can display variable values and change them from the command line as shown in Example 8, “Creating a Tailoring That Checks for a Password Length of 13,” on page 30, or from the pick screen of the curses editor, as described in “How to Create a Tailoring From a Compliance Benchmark” on page 19.

▼ How to Select a Non-Default Value for a Rule in a Tailoring

Before You Begin You must be assigned the Compliance Assessor rights profile to create a tailoring that can be added to the assessment store. For more information, see “Rights to Run the `compliance` Command” on page 12 and “Using Your Assigned Administrative Rights” in *Securing Users and Processes in Oracle Solaris 11.3*.

1. **Create a tailoring that modifies the value of a rule.**

   ```
   $ compliance tailor -t tailoring
   ```

```
*** compliance tailor: Can't get existing tailor "tailoring", initializing
tailoring:tailoring> set benchmark=benchmark
```

2. **List the rules in the benchmark or profile that contain variables.**

```
tailoring:tailoring> values
OSCV-nnnnn (summary):  value
OSCV-nnnnn (summary):  value
...
#
```

3. **Change the value of a rule that contains a variable.**

```
tailoring:tailoring> include OSC-nnnnn
tailoring:tailoring> value OSCV-nnnnn=value
```

4. **Commit your changes and test.**

```
tailoring:tailoring> commit
tailoring:tailoring> exit
# compliance assess -t tailoring
Assessment will be named 'tailoring.date'
Title   Rule title
Rule    OSC-nnnnn
Result  pass
```

Example 8 Creating a Tailoring That Checks for a Password Length of 13

1. Change the default password length according to site requirements.

   Change the PASSLENGTH value in the /etc/default/passwd file.

```
## /etc/default/passwd file
##PASSLENGTH=8
PASSLENGTH=13
```

2. Create a tailoring from the solaris benchmark.

```
$ pfexec compliance tailor -t passwdLength13Test
*** compliance tailor: Can't get existing tailor "passwdLength13Test", initializing
tailoring:passwdLength13Test> set benchmark=solaris
```

3. Display the rules in the solaris benchmark that contain variables and their possible values.

```
tailoring:passwdLength13Test> values -v
OSCV-19500 (gdm service):  _disabled_ /disabled|enabled/
OSCV-37500 (NFS client service):  _disabled_ /disabled|enabled/
OSCV-46000 (Minimum Password Length):  6 <= _8_ <= 255 /6|8|14/
```

```
OSCV-47000 (Minimum Password Character Difference):  1 <= _3_ /3/
OSCV-48000 (Minimum Password Lower-Case Character Count):  0 <= _0_ /0|1/
OSCV-49000 (Minimum Password Special Character Count):  0 <= _0_ /0|1/
```

The output shows that the minimum password length that rule OSC-46000 can check for is `6` and the maximum is `255`. The current value is `8`.

4. Set the rule to check for a minimum password length of `13`.

```
tailoring:passwdLength13Test> include OSC-46000
tailoring:passwdLength13Test> value OSCV-46000=13
tailoring:passwdLength13Test> commit
tailoring:passwdLength13Test> exit
$
```

5. Test the tailoring.

```
$ compliance assess -t passwdLength13Test
Assessment will be named 'passwdLength13Test.2015-10-10,10:10'
Title   Passwords must be at least 13 characters long
Rule    OSC-46000
Result  pass
```

Running Assessments at Regular Intervals

The `compliance:default` SMF service enables you to run assessments at regular intervals. When you enable the service, it regularly runs an assessment against the system's default policy. You can modify the default policy and set a different schedule.

The `compliance:default` service is delivered disabled. To run regular assessments, you enable the service. To schedule a policy assessment that is not the default, you perform two operations:

1. Change the system's policy to a different benchmark, profile, or tailoring by running the `compliance set-policy` command
2. Modify the assessment schedule by using the `svccfg` command to add or modify one or more `scheduled` service properties of the `compliance:default` service.

For more information about scheduled services, review the following:

- Chapter 4, “Configuring Services” in *Managing System Services in Oracle Solaris 11.3*
- “Scheduling Executions of a Scheduled Service Start Method” in *Developing System Services in Oracle Solaris 11.3*
- `svc.periodicd`(1M) man page.

How to Schedule a Regular Assessment of a System Using Its Default Policy

Before You Begin You must be assigned the Compliance Assessor rights profile to schedule assessments that can be added to the assessment store. To run the `svccfg`, you must be assigned the Service Configuration rights profile. For more information, see "Rights to Run the `compliance` Command" on page 12 and "Using Your Assigned Administrative Rights" in *Securing Users and Processes in Oracle Solaris 11.3*.

1. Change the default policy to the correct policy if needed.

a. List the default policy.

```
$ compliance get-policy
Benchmark:      solaris
Profile:        Baseline
Tailoring:
```

b. List the available benchmarks, profiles, and tailorings.

```
$  compliance list -p
pci-dss:        Solaris_PCI-DSS
solaris:        Baseline, Recommended
$  compliance list -t
        basic
        RKerberos
```

You can also use the `compliance tailor list` command to list the available tailorings.

c. Set the correct default policy for this system.

In this example, you assign an existing tailoring as the default policy.

```
$ pfbash ; compliance set-policy -t RKerberos
$ compliance get-policy
Benchmark:
Profile:
Tailoring:    RKerberos
```

2. Before changing to a new schedule, return the schedule to the default schedule.

```
$ svccfg -s compliance:default delcust
$ svccfg -s compliance:default listprop scheduled
 scheduled           schedule
 scheduled/frequency integer     1
```

```
 scheduled/interval  astring     week
```

3. **Set the new schedule and list it.**

```
$ svccfg -s compliance:default setprop scheduled/property  =  type:    value
$ svccfg -s compliance:default listprop scheduled
scheduled           schedule
scheduled/frequency integer     1
scheduled/interval  astring     week
scheduled/property     type       value
$ svcadm refresh compliance:default
```

Several properties are defined for scheduled services, such as `scheduled/hour` and `scheduled/day_of_week`. For examples of these properties, see Example 11, “Scheduling the Weekday and Hour of an Assessment,” on page 34 and Example 12, “Running a Policy Assessment Daily,” on page 35. For more information, see “How to Schedule a Periodic or Scheduled Service” in *Managing System Services in Oracle Solaris 11.3* and the `svc.periodicd`(1M).

4. **Refresh the service.**

```
$ svcadm refresh compliance:default
```

5. **Enable the service if it is not enabled.**

```
$ svcs -x compliance:default
svc:/application/security/compliance:default (Scheduled compliance assessment)
 State: disabled since Fri Jan  8 10:10:10 2016
Reason: Disabled by an administrator.
   See: http://support.oracle.com/msg/SMF-8000-05
   See: compliance(1M)
   See: /var/svc/log/application-security-compliance:default
Impact: This service is not running.
$ svcadm enable compliance:default
$ svcs compliance:default
STATE          STIME    FMRI
online         10:21:22 svc:/application/security/compliance:default
```

6. **Verify that the initial run is scheduled.**

```
$ svcs -o lrun,nrun compliance:default
LRUN     NRUN
         Jan_08
```

7. **After the initial run, verify that the assessment ran.**

```
$ svcs -o lrun,nrun compliance:default
LRUN     NRUN
02:10:10 Jan_08
```

8. **(Optional) View the assessment in a browser.**

   a. **Locate the report.**

      ```
      $ pfexec compliance report
      /var/compliance/assessments/solaris/tailoring1/tailoring1.2016-01-03,02:11/report.html
      ```

   b. **To view the report, type the file location into the browser.**

      ```
      file:///var/compliance/assessments/solaris/tailoring/tailoring.2016-01-03,02:11/report.
      html
      ```

Example 9 Setting the Default Policy to a Benchmark or Profile

This example sets the default policy to the `Recommended` profile of the `solaris` benchmark.

```
$  compliance list -p
pci-dss:        Solaris_PCI-DSS
solaris:        Baseline, Recommended
$ compliance set-policy -b solaris -p Recommended
$ compliance get-policy
Benchmark:      solaris
Profile:        Recommended
Tailoring:
```

Example 10 Setting the Default Policy to an Installed Tailoring

This example sets the default policy to a tailoring that was installed as a package. This example assumes that `RKerberos` was installed as a package on this system.

```
$  compliance set-policy -b solaris -t RKerberos
$ compliance get-policy
Benchmark:    solaris
Profile:      Recommended
Tailoring:    RKerberos
```

For the contents of the `RKerberos` tailoring, see Example 5, “Creating a Kerberos Tailoring From the `Recommended` Profile,” on page 24.

Example 11 Scheduling the Weekday and Hour of an Assessment

In this example, the `root` role adds to the default schedule by specifying the day of the week and the hour that the assessment should run. After refreshing the service, `root` checks that the new schedule is valid.

```
$ svccfg -s compliance:default setprop scheduled/day  =  astring:  Sunday
```

```
$ svccfg -s compliance:default setprop scheduled/hour  =  integer:  2
$ svccfg -s compliance:default listprop scheduled
scheduled           schedule
scheduled/frequency integer     1
scheduled/interval  astring     week
scheduled/day       astring     Sunday
scheduled/hour      integer     2
$ svcadm refresh compliance:default
$ svcs -x compliance:default
svc:/application/security/compliance:default (Scheduled compliance assessment)
 State: online since Fri Jan 08 11:11:11 2016
 ...
```

Example 12 Running a Policy Assessment Daily

In this example, the `root` role changes the assessment to run daily after 2 a.m. After refreshing the service, `root` checks that the new schedule is in effect.

```
$ pfbash ; svccfg -s compliance:default setprop scheduled/interval  =  astring:  day
$ svccfg -s compliance:default setprop scheduled/hour  =  integer:  2
$ svcadm refresh compliance:default
$ svccfg -s compliance:default listprop scheduled
scheduled           schedule
scheduled/frequency integer     1
scheduled/interval  astring     day
scheduled/hour      integer     2
$ svcs compliance:default
STATE          STIME    FMRI
online          11:11:11 svc:/application/security/compliance:default
$ svcs -o lrun,nrun compliance:default
LRUN     NRUN
-        Jan_08
```

How to Return to the Default Schedule for Running Assessments

Before You Begin You must be assigned the Service Configuration rights profile to run the `svccfg` command. For more information, "Using Your Assigned Administrative Rights" in *Securing Users and Processes in Oracle Solaris 11.3*.

1. List your customizations.

```
$ pfbash ; svccfg -s compliance:default listcust
general/enabled                   boolean     admin                true
```

```
scheduled/day                       astring     admin                Sunday
scheduled/hour                      integer     admin                2
periodic_restarter                  framework   admin
periodic_restarter/scheduled        time        admin                1111224444
periodic_restarter/next_run         time        admin                1111224444
```

2. **Return the service to the default.**

```
$ svccfg -s compliance:default delcust
$ svccfg -s compliance:default listprop scheduled
scheduled           schedule
scheduled/frequency integer     1
scheduled/interval  astring     week
```

See Also "How to Schedule a Periodic or Scheduled Service" in *Managing System Services in Oracle Solaris 11.3*

Troubleshooting If a scheduled compliance run cannot run at its scheduled start time, future scheduled runs may also fail. To restart the schedule, clear the maintenance state, then disable and enable the `compliance:default` service instance.

```
$ svcadm clear compliance:default; svcadm disable compliance:default; svcadm
enable compliance:default
```

♦ ♦ ♦ CHAPTER 2

Administering Compliance to Critical Security Updates

This chapter describes how to determine whether your system has the latest critical patch updates from Oracle Solaris as reported by CVE number (CVE ID). It covers the following topics:

Administering CVE Updates in Oracle Solaris

Systems that contain the most recent security fixes provide a more secure computing environment. Oracle Solaris provides online access to the Common Vulnerabilities and Exposures (CVE) list and other security fixes. The `pkg` command has options to search for CVE updates.

Monitoring CVE Status in Oracle Solaris

You can monitor the status of critical updates to Oracle Solaris packages by following the information at the Oracle Critical Patch Updates, Security Alerts and Third Party Bulletin web site. You should apply critical patch updates without delay.

Locating the Packages That Have CVE Updates in Oracle Solaris

The Oracle Solaris Support package repository contains metadata for tracking security vulnerability fixes by the assigned CVE ID. Oracle Solaris creates a package of this metadata from the Oracle bug database. After installing the package, you can easily determine whether your system has all the known and required security vulnerability fixes. You do not need to derive this information from other sources. Using the Oracle bug database as your source is critically important because sometimes Oracle Solaris fixes a bug in an upstream Free and Open Source (FOSS) component by patching the code rather than by generating a new version of the component.

The metadata package from the Oracle bug database, `pkg:/support/critical-patch-update/solaris-11-cpu`, covers the `entire` dependency hierarchy. All packages that were changed for a particular CVE fix are dependencies of the `solaris-11-cpu` package. They are "optional" dependencies, therefore they are updated if they are already installed, but not installed if the software that is being fixed is not already installed.

The metadata package enables retrospective updates to the critical patch update (CPU) metadata where a shipped version already contains the fix for a given CVE ID. When Oracle Solaris publishes a new CPU, it also publishes a new version of the package to the Oracle Solaris support repository plus the new package versions that contain the fixes.

The version format for the CPU package is `@`*YYYY*`.`*MM*`-`*VV* where *VV* is usually a low number, as in the CPU package `solaris-11-cpu@2014.10-1`. This format enables Oracle Solaris to republish critical patch updates within the same month. Note that the day of the month (*DD*) is not part of the version format.

You can search the metadata by using either the Oracle Solaris Support package repository web site or the command-line interface. You can search for cases where a given CVE ID applies to multiple packages and also where a given package version contains fixes for multiple CVE IDs.

Installing the CPU Package

Your Oracle Solaris 11 systems do not have the `solaris-11-cpu` package installed by default, because this package is higher in the dependency hierarchy than the `entire` package. You must explicitly install the CPU package.

```
# pkg install solaris-11-cpu
```

After installation, the CPU package updates the system to the SRU version of the CPU. The updating includes all package updates between the SRU of the system and the SRU version of the CPU. For more information and examples, see "Applying Support Updates" in *Adding and Updating Software in Oracle Solaris 11.3* and "Critical Patch Update Packages" in *Adding and Updating Software in Oracle Solaris 11.3*.

Managing CVE Updates From the Command Line

The examples in this section show how to use the command line to find CVE information.

EXAMPLE 13 Several Ways of Listing the Packages That Contain Fixes to a CVE ID

When you know the CVE ID, you can use it to find the packages that contain the fix for it. The following searches find the fix for the `bash` Shellshock software bug.

- The `pkg search` command searches all configured repositories and the local system for the CVE ID. The output lists which packages and versions contain the fix and which CPU delivers it. Note the use of the trailing colon (`:`) in the search to indicate a missing field.

```
$ pkg search CVE-2014-7187:
INDEX         ACTION VALUE                                                PACKAGE
CVE-2014-7187 set    pkg://solaris/shell/bash@4.1.11,5.11-0.175.2.2.0.8.0 pkg:/
support/critical-patch-update/solaris-11-cpu@2015.8-1
CVE-2014-7187 set    pkg://solaris/shell/bash@4.1.11,5.11-0.175.2.2.0.8.0 pkg:/
support/critical-patch-update/solaris-11-cpu@2015.7-3
...
CVE-2014-7187 set    pkg://solaris/shell/bash@4.1.11,5.11-0.175.2.2.0.8.0 pkg:/
support/critical-patch-update/solaris-11-cpu@2014.10-1
CVE-2014-7187 set    pkg://solaris/shell/bash@4.1.11,5.11-0.175.2.3.0.4.0 pkg:/
support/critical-patch-update/solaris-11-cpu@2014.10-1
```

- Without the trailing colon, the `pkg search` command lists all `solaris-ll-cpu` package versions, but does not list the `bash` package that contains the fix.

```
$ pkg search CVE-2014-7187
  INDEX   ACTION VALUE          PACKAGE
info.cve  set    CVE-2014-7187  pkg:/support/critical-patch-update/solaris-11-
cpu@2015.8-1
info.cve  set    CVE-2014-7187  pkg:/support/critical-patch-update/solaris-11-
cpu@2014.4-1
...
```

```
info.cve set CVE-2014-7187 pkg:/support/critical-patch-update/solaris-11-
cpu@2014.10-1
```

- The following command displays the CVE ID, the package that contains the fix, and `solaris-11-cpu` package version:

```
$ pkg search -Ho name,value,pkg.shortfmri CVE-2014-7187:
CVE-2014-7187   pkg://solaris/shell/bash@4.1.11,5.11-0.175.2.2.0.8.0    pkg:/support/
critical-patch-update/solaris-11-cpu@2015.8-1
...
CVE-2014-7187   pkg://solaris/shell/bash@4.1.17,5.11-0.175.2.5.0.2.0    pkg:/support/
critical-patch-update/solaris-11-cpu@2015.7-1
...
CVE-2014-7187   pkg://solaris/shell/bash@4.1.11,5.11-0.175.2.2.0.8.0    pkg:/support/
critical-patch-update/solaris-11-cpu@2014.10-1
```

- The `pkg contents -r` command searches the repository, not the local system, for the packages that fix the `bash` Shellshock software bug.

```
$ pkg contents -Hro value -t set -a name=CVE-2014-7187 solaris-11-cpu
pkg://solaris/shell/bash@4.1.11,5.11-0.175.2.2.0.8.0
pkg://solaris/shell/bash@4.1.11,5.11-0.175.2.3.0.4.0
pkg://solaris/shell/bash@4.1.17,5.11-0.175.2.5.0.2.0
```

Because SRUs and CPUs are cumulative, the fix is available after being installed once.

EXAMPLE 14 Showing When a CVE Fix Was First Available

This example shows that the fix for the `bash` Shellshock software bug was first available for this system in the `solaris-11-cpu@2014.4-1` package and in every following SRU.

```
$ pkg search -po pkg.shortfmri CVE-2014-7187
PKG.SHORTFMRI
pkg:/support/critical-patch-update/solaris-11-cpu@2014.4-1
pkg:/support/critical-patch-update/solaris-11-cpu@2015.1-1
pkg:/support/critical-patch-update/solaris-11-cpu@2015.1-2
...
```

EXAMPLE 15 Listing the CVE IDs in a Critical Patch Update

This example shows how to display every fixed CVE in the latest CPU.

```
$ pkg contents -rHo value -a name=info.cve solaris-11-cpu@latest
CVE-1999-0103
CVE-2002-2443
CVE-2003-0001
```

```
CVE-2004-0230
...
CVE-2015-5477
...
```

EXAMPLE 16 Verifying That the Latest CPU Is Installed

To determine the status of the latest `solaris-11-cpu` package, use the `pkg list` command.

```
$ pkg list -af solaris-11-cpu@latest
NAME (PUBLISHER)                                  VERSION                    IFO
support/critical-patch-update/solaris-11-cpu      2015.8-1                   ---
```

Because the `i` flag is not in the `I` column, the latest CPU is not installed.

EXAMPLE 17 Verifying That a Fix for a CVE ID Is Installed

To verify that you installed a fix for a specific CVE ID, search your installed packages for the CVE ID. If it is not installed, no output displays. The `pkg search -l` command searches the local disk only.

```
# pkg search -l CVE-2014-7187
INDEX      ACTION VALUE         PACKAGE
info.cve   set    CVE-2014-7187 pkg:/support/critical-patch-update/solaris-11-cpu@2014.
10-1
```

For more information about options to the `pkg` command, see the `pkg(1)` man page.

♦ ♦ ♦ APPENDIX A

Compliance Reference

The compliance area of computer security assumes familiarity with many standards, acronyms, and processes. The following lists of terms and references are provided for your convenience.

Compliance Utilities

The following programs implement compliance assessment and reporting:

- Security Content Automation Protocol (SCAP)
- SCAP tools (OpenSCAP)
- Open Vulnerability and Assessment Language (OVAL)
- eXtensible Configuration Checklist Description Format (XCCDF)

Compliance Standards

The following bodies provide compliance guides, standards, or laws:

- Center for Internet Security (CIS)
- Defense Information Systems Agency-Security Technical Information Guides (DISA-STIG)
- Federal Information Security Management Act (FISMA)
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)

  Health Information Technology for Economic and Clinical Health Act (HITECH) (Modifications to the HIPAA Rules)
- Payment Card Industry-Data Security Standard (PCI DSS)
- Sarbanes Oxley (SOX)

Index