# Citi Architecture and Technology Engineering (CATE)
## CATE CitiSystems Server and OperatingEnvironment Engineering

# Requirements, Testing & Release Notes

| | |
|---|---|
| Project Name: | **Solaris 10 - VTM Solutions - 2017Q4-1** |
| Project ID: | **CAT170083126** |
| Document Version: | 1.0 |
| Date Published: | January, 05 2018 |

# TABLE OF CONTENTS

# 1 OVERVIEW

## 1.1 Script Lite Certification Types

**Product Certification** - A minor upgrade for existing infrastructure or platform technology standard that does not impact the security model. This may include product hardware and/or product software.

**DO NOT DELETE ANY SECTIONS FROM THIS DOCUMENT. PLEASE USE SHORT DESCRIPTION FOR SECTIONS AND DETAILS THAT DO NOT APPLY.**

**Vulnerability Threat Management (VTM)** - A minor upgrade due to a vulnerability (via VTMAS) for an existing infrastructure or platform technology standard that does not impact the security model. VTM related work can be a vendor software fix and/or configuration changes. Please note if the vulnerability has a major impact to the architecture and/or security model then the TDLC Create/Maintain project type must be used.

For either certification type any sections marked Not Applicable (N/A) must be accompanied with reason why the particular item does not apply.

- Example: N/A - This effort is for VTM vulnerability remediation and solution consisted of configuration change.

Please hover over **Choose an item**, left click and use the drop down menu below to identify certification type.

**Vulnerability Threat Management (VTM)** ← **Hovering will allow choosing SL cert type**

## 1.2 Document Purpose

The purpose of the template is to provide a standard document structure for completing all requirements for Solaris 10 - VTM Solutions - 2017Q4-1

## 1.3 Revision History

**Update the document history each time a draft is issued for review.**

| Date | Version | Author | Author Contact | Change (Topic, Section Page) |
|------|---------|--------|----------------|------------------------------|
| November 09, 2017 | 1.0 | S Senthil | senthil.shanmugavelu@citi.com | Initial RFT |
| January 05, 2018 | 1.1 | S Senthil | senthil.shanmugavelu@citi.com | RFP |

## 1.4 Relevant Links

**Provide titles and links to documentation supporting the product. These documents can be a combination of vendor documents and vendor sites (for example, Cisco, VMware). Wherever possible, vendor documents should be posted to internal sites to make sure they are accessible.**

**External References (E.g., Vendors etc.)**

| Document | URL |
|---|---|
| Oracle Critical Patch Update Advisory – October 2017 | http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html |
| | |
| | |

**Internal References**
**Provide a list of internal documents that have been used as an input to this document. Include design and configuration guidelines in this section.**
**Provide the document name, version number and publication date. Provide hyperlinks to each document as well.**

| Document | Version | Date |
|---|---|---|
| CATE Solaris Product Details | | |
| RFP | Release For production: Solaris 10 VTM Solution 2017Q3-1 | V1 | 10/23/2017 |
| RFP | Release For production: Solaris 10 VTM Solution 2017Q2-1 | V1 | 06/23/2017 |
| RFP | Release For production: Solaris 10 VTM Solution 2017Q1-1 | V1 | 03/31/2017 |
| RFP | Release For production: Solaris 10 VTM Solution 2016Q4-1 | V1 | 12/14/2016 |
| RFP | Release for Production: Solaris 10 Kernel Update 7.7 | KU7.7 | 04/28/2016 |
| RFP | Release for Production: VTM-Solutions for Solaris 10 | VTM 2.11 | 03/28/2016 |

# 2 REQUIREMENTS, TESTING & RESULTS

## 2.1 Overview and Product Requirements

This new patchset for Solaris 10 resolves new vulnerabilities identified by VTM's ID [79135, 79150, 79165, 71260, 79180, 71266, 71272, 75004, 79212, 79237, 79252, 79275, 79305, 79329,  79374, 79413] refer section 2.2 Vulnerability Threat Management (VTM) Requirements in this document for details of all VTMs solutions contained in this patchset

This new bundle will accumulate all new VTM solutions with Live upgrade (recommended) or single user install requirement. This patchset MUST  be applied to all installed Solaris 10 SOE systems

CATE does not support and has never supported a Veritas encapsulated root disks on Solaris 10. If your system has an encapsulated root disk you will need to remediate immediately. It is impossible for CATE to track every issue on unsupported configurations as CATE does not do testing with unsupported configurations.

## 2.2 Cloud Architecture Review Team Assessment (CART)

**NOTE**: If you created your Project on or after June 5, 2017, the following assessment will be captured in the Planview Tool within the required Combined Compliance Assessment Lifecycle screen. If you created your project before June 5, 2017, you must complete this section.

**Assessment Question:** Does your project involve or have any elements associated with External Hosting, whether traditional or Cloud?

- Externally Hosted (any system or service with Citi Data stored or processed outside Citi perimeter.) or Dedicated (Dedicated refers to physical server hardware dedicated to Citi use, ideally in a dedicated Citi cage) or Single Tenant Cloud or Lab/POC with no Citi data.
- Shared Cloud, no confidential or higher data stored or processed.
- Shared Cloud, confidential or higher data stored or processed.

If you answered No in the below table, then you do not need to contact the CART Team.

If you answered Yes in the below table, you must go to the CART SharePoint site and initiate a request for review. Ensure that a CART Approval Email or Waiver is obtained and uploaded to the Product Registration Activity in Planview before releasing to Production and marking the Project as Completed.

| CART Assessment | Yes or No |
|---|---|
| Does your project involve or have any elements associated with External Hosting, whether traditional or Cloud? | No |

| CART Assessment | Yes or No |
|---|---|
| If you answered Yes, have you contacted the CART Team and requested a Formal Approval or Waiver? | NA |

## 2.3 Mobile Architecture Review Team Assessment (MART)

**NOTE**: If you created your Project on or after June 5, 2017, the following assessment will be captured in the Planview Tool within the required Combined Compliance Assessment Lifecycle screen. If you created your project before June 5, 2017, you must complete this section.

**Assessment Question**: Does your project or development activity includes any downloadable or installed component that runs/resides on a customer/end user device (mobile, tablet, laptop, etc.) then review and approval by the Mobile Architecture Review Team (MART) is required before releasing into production.

If you answered No, then you do not need to contact the MART Team.

If you answered Yes in the below table, you must go to the MART SharePoint site and initiate a request for review. Ensure that a MART Approval Email or Waiver is obtained and uploaded to the Product Registration Activity in Planview before releasing to Production and marking the Project as Completed.

| MART Assessment | Yes or No |
|---|---|
| Does your project or development activity includes any downloadable or installed component that runs/resides on a customer/end user device (mobile, tablet, laptop, etc.)? | No |
| If you answered Yes, have you contacted the MART Team and requested a formal approval or Waiver? | NA |

## 2.4 Legal and Regulatory Assessment

**NOTE**: If you created your Project on or after June 5, 2017, the following assessment will be captured in the Planview Tool within the required Combined Compliance Assessment Lifecycle screen. If you created your project before June 5, 2017, you must complete this section.

**Assessment Question**: Does your project involve any of the following Legal and/or Regulatory Compliance elements?

- Electronic communications with clients by Citi employees (including e-mail, IM or other electronic messaging)
- Social networking related projects

- Employee telephone recordings

- Internal websites, wikis or other means by which Citi employees may be able to post/share information

- Any systems related to trading

- Data archiving or records management

If you answered No in the table below, then you do not need to contact your Control Officer or obtain a Legal and Regulatory review.

If you answered Yes in the below table, you must contact your Control Officer and request a Legal and Regulatory review. Ensure that the Legal and Regulatory finding or Approval Email to proceed is obtained in writing and uploaded to the Product Registration Activity in Planview before releasing to Production and marking the Project as Completed.

| Legal and Regulatory Assessment | Yes or No |
|---|---|
| Does your project involve any of the following Legal and and/or Regulatory Compliance elements?<br><br>• Electronic communications with clients by Citi employees (including e-mail, IM or other electronic messaging)<br><br>• Social networking related projects<br><br>• Employee telephone recordings<br><br>• Internal websites, wikis or other means by which Citi employees may be able to post/share information<br><br>• Any systems related to trading<br><br>• Data archiving or records management | No |
| If you answered Yes, have you contacted your Control Officer and requested a Legal and Regulatory review. | NA |

## 2.5 Vulnerability Threat Management (VTM) Requirements (Only if VTM related work)

| VTM ID | CVE ID | CVE description | Vendor defect ID | Patch Number |
|---|---|---|---|---|
| 79135 | CVE-2017-10388 | Oracle Java SE CVE-2017-10388 Remote Security Vulnerability | BID-101321 | 152076-71 152077-71 |

| 79150 | CVE-2017-10346 | Oracle Java SE CVE-2017-10346 Remote Security Vulnerability | BID-101315 | 152076-71 152077-71 |
|---|---|---|---|---|
| 79165 | CVE-2017-10285 | Oracle Java SE CVE-2017-10285 Remote Security Vulnerability | BID-101319 | 152076-71 152077-71 |
| 71260 | CVE-2017-6464 | NTP CVE-2017-6464 Denial of Service Vulnerability | BID-97050 | 143725-11 |
| 79180 | CVE-2017-10274 | Oracle Java SE CVE-2017-10274 Remote Security Vulnerability | BID-101333 | 152076-71 152077-71 |
| 71266 | CVE-2017-6463 | NTP CVE-2017-6463 Denial of Service Vulnerability | BID-97049 | 143725-11 |
| 71272 | CVE-2016-9042 | NTP CVE-2016-9042 Denial of Service Vulnerability | BID-97046 | 143725-11 |
| 75004 | CVE-2017-3629 | Oracle Solaris CVE-2017-3629 Local Privilege Escalation Vulnerability | BID-99150 | 147793-22 150400-55 |
| 79212 | CVE-2017-10357 | Oracle Java SE CVE-2017-10357 Remote Security Vulnerability | BID-101355 | 152076-71 152077-71 |
| 79237 | CVE-2017-10349 | Oracle Java SE CVE-2017-10349 Remote Security Vulnerability | BID-101348 | 152076-71 152077-71 |
| 79252 | CVE-2017-10348 | Oracle Java SE CVE-2017-10348 Remote Security Vulnerability | BID-101354 | 152076-71 152077-71 |
| 79275 | CVE-2017-10293 | Oracle Java SE CVE-2017-10293 Remote Security Vulnerability | BID-101338 | 152076-71 152077-71 |
| 79305 | CVE-2017-10355 | Oracle Java SE and JRockit CVE-2017-10355 Remote Security Vulnerability | BID-101369 | 152076-71 152077-71 |
| 79329 | CVE-2017-10347 | Oracle Java SE and JRockit CVE-2017-10347 Remote Security Vulnerability | BID-101382 | 152076-71 152077-71 |
| 79374 | CVE-2017-10281 | Oracle Java SE and JRockit CVE-2017-10281 Remote Security Vulnerability | BID-101378 | 152076-71 152077-71 |
| 79413 | CVE-2016-10165 | lcms2 CVE-2016-10165 Out-of-Bounds Read Denial of Service Vulnerability | BID-95808 | 152076-71 152077-71 |

## 2.6 Testing Scope

This test plan will make sure that all the VTM solutions has been tested and executed properly.

This table is to identify what categories will be tested. Test Categories are derived from CSTLC. Section 2.9 will capture specific tests that align to this table. Please indicate Yes/No and provide details in Table 1, Section 2.9.1.

| Test Category | Definition | Test Category Required (Yes or No) |
|---|---|---|
| System Integration Testing (Including: Interface Testing, Batch Testing) | System integration testing (SIT) is a testing process that exercises a software system's coexistence with others. With multiple integrated systems, assuming that each have already passed system testing, SIT proceeds to test their required interactions. Following this, the deliverables are passed on to acceptance testing. System Integration Testing verifies combined functionality. | Yes |
| Functional Testing | Testing software based on its functional requirements. It ensures that the program physically works the way it was intended and all required menu options are present. It also ensures that the program conforms to the industry standards relevant to that environment; for example, in a Windows program, pressing F1 brings up help. In this type of testing, the system is validated for its functional behavior. Functional testing does not deal with internal coding of the project. | Yes |
| VTM Testing | VTM related testing ensures that you have reviewed the CVEs and based on the impact and availability, feasible testing can be included in this section.  (can include VTM scans and or tools available) | Yes |
| Non-Functional Testing | Testing the attributes of a component or system that do not relate to functionality, e.g. reliability, efficiency, usability, maintainability, and portability. | No |
| Technology Testing | Refers to all testing performed by the technology staff. | Yes |

| Other Testing | User Acceptance Testing, exploratory testing. This could include possible Operational, Regional and user feedback. | No |
|---|---|---|

## 2.7 Testing Constraints

Test environment must meet the requirements detailed given in section 3.3 Pre-requisites

## 2.8 Testing Dependencies

- The patchset MUST be installed in single-user mode if not updating an ABE (Alternate boot environment).

- The patchset MUST be installed from a local permanent filesystem such as /var/tmp, if not updating an ABE, the Installation from NFS mounts will not supported on single user mode and the process involves a reboot.

## 2.9 Test Specifications, Defect Tracking

### 2.9.1 Test Category Tests

Table 1

| Test Category (Based on section 2.3 table) | Test specification | Expected Results | Actual Results | Pass / Fail |
|---|---|---|---|---|
| System Integraion Testing,Functional Testing,VTM Testing, Technology Testing | Install Patchset on solaris 10 server. Verify file sum and permissions | Patchset installed successfully. Permissions and sums verified | Patchset installed successfully. Permissions and sums verified | Pass |
| System Integraion Testing,Functional Testing, VTM Testing, Technology Testing | Install Patchset, confirm the Patchset installation, verify the solaris 10 functionality (Login function and connectivity) | Login functions, Patchset reflected by Solaris10 server as installed | Login functions, Patchset reflected by Solaris10 server as installed | Pass |

| Test Category (Based on section 2.3 table) | Test specification | Expected Results | Actual Results | Pass / Fail |
|---|---|---|---|---|
|  |  |  |  |  |

## 2.9.2 Defect Tracking Log

There are no defects identified as part of the testing for this work effort

| Defect ID | Description | Severity | Will the Defect Be Fixed (Y/N) | Comments (Additional detail about the defect) |
|---|---|---|---|---|
|  |  |  |  |  |
|  |  |  |  |  |

# 3 RELEASE DETAILS

## 3.1 Release Details

| | |
|---|---|
| **Product Vendor** | Oracle |
| **Product Name** | Solaris 10 |
| **CTC Product ID** | 7058 |
| **CTC Version ID(s)** | 21782 |
| **Product Homepage** | https://catecollaboration.citigroup.net/domains/platstor/osunix/wpages/ProductDetail.aspx?Name=Solaris&Publish=1 |

## 3.2  Source Code Management Repository

This section should include location of the Source Code (Custom files/Scripts) used for this release.
If Source Code was not used in the Software or Package, indicate "Not Applicable" (N/A) and provide explanation:

Not Applicable : No custom files/scripts have been used in this release.

| Repository Name | Repository URL | Source Code Identifier |
|---|---|---|
| 1.   NA | NA | NA |
| 2.   NA | NA | NA |

## 3.3 Software and Packages –

| Platform | Package Name | Repository | Size(bytes) | MD5 / SHA1 / SHA256 (if applicable) |
|---|---|---|---|---|
| Sparc – Solaris 10 | S10-Patches-2017-Q4.tgz | stealth | 2481131749 | 664b1c3840ee69751a61daf624ce3aa4 / 4c40115711300c2fc9005544590cc3298e1f87be / NA |

**Stealth**: NFS://net/stealth.nam.nsroot.net/export1/home1.localhost/sw/PKG

## 3.4 Pre-requisites

1.  When installing this patchset to an alternate boot enviornment , the install script may stop and notify the user of the need to invoke the script with the "--apply-prereq" flag to ensure appropriate levels of various patches (including the patch utility patches) are applied to the running system. Please follow the instruction mentioned in the **step 4**  from Live Upgrade Install. Following patchset may install while doing this installation  119254-93 138215-03 148336-03 125555-16


2.  Package need 3 GB space while copying from Stealth and 7 Gb free space while extracting the zip file to local directory.

3.   Non-Global zones should be in HALT (installed) state ,while installing this patchset on **single usermode . No change in LIVE UPGRADE Installation**

# 4 INSTALL AND/OR CONFIGURATION INSTRUCTIONS

## 4.1 Pre-installation steps for Solaris 10

**(*Highly Recommended*)**

In order to save time, the SA can perform the following steps prior to the installation, as regular user:

**Method 1:** Copy tar file into local directory( Need 10 GB free space to copy and extract the zip file)

1. Identify the stealth and copy the zip file

```
cd /net/stealth.nj.ssmb.com/export1/home1.localhost/sw/PKG
```

```
scp S10-Patches-2017-Q4.tgz <TargetHost>:/var/tmp
```

2. On each applicable host, extract the Patchset. Check that this filesystem is local and not "tmpfs"

```
cd /var/tmp
```

```
df –nl
```

**Package need 7 Gb free space while extracting the zip file (Assume pkg copied into /var/tmp)**.

```
gzip –dc  /var/tmp/S10-Patches-2017-Q4.tgz  | tar xf  –
```

**Method 2:**  Extract from an NFS share, the local disk space requirements can be reduced by not copying the tar file locally

```
cd /var/tmp
```

```
/var/tmp#  gzcat  /net/some/nfs/share/S10-Patches-2017-Q4.tgz |  tar –xf  –
```

## 4.2 Live Upgrade Install:

When possible using Live Upgrade to install the Solaris 10 Recommended Patchset will save time and reduce downtime. Live Upgrade also has a reliable backout method that SA can simply revert to the previous boot environment to back out patch changes. Live Upgrade can be used on systems with Solaris Volume Manger however CATE recommends moving root disks to ZFS wherever possible. The following instructions are for ZFS based root disks. More info on SVM based root disk installation instructions can be found at Best Practice: Patching with Solaris Live Upgrade.

1.  Create a alternate boot environment

```
# lustatus
Boot Environment  Is          Active   Active      Can     Copy
Name              Complete    Now      On Reboot   Delete  Status
----------------------------------------- -------- ------ --------- ------ ----------
S10_0910_US       yes         yes      yes         no      -
```

```
# lucreate -n S10-Patches-2017-Q4
Analyzing system configuration.
Updating boot environment description database on all BEs.
…..
Population of boot environment < S10-Patches-2017-Q4> successful.
Creation of boot environment < S10-Patches-2017-Q4> successful          -
```

2.  Mount the ABE(alternate boot environment) into a filesystem.

```
# lumount S10-Patches-2017-Q4 /a
/a
```

3.  For installation to an Alternate Boot Environment, the unpacked version can be on an NFS share or you can follow the Method 1/Method 2 in Pre installation steps to extract the zip file into local directory

```
NFS share:
cd /net/some/nfs/share/S10-Patches-2017-Q4

Local Directory:
cd /var/tmp
```

4.  Install the prerequisite packages

```
bash-3.2#  ./installpatchset --apply-prereq

The Server is IDENBUILD environment.
Server hardware is supported.  Patch installation proceeding.



Setup ...


CPU OS Patchset 2017/10 Solaris 10 SPARC (2017.10.12)

Application of patches started : 2017.10.26 20:48:05

Applying 120900-04 ( 1 of 10) ... skipped
Applying 121133-02 ( 2 of 10) ... skipped
Applying 119254-93 ( 3 of 10) ... skipped
Applying 119317-01 ( 4 of 10) ... skipped
Applying 121296-01 ( 5 of 10) ... skipped
Applying 138215-03 ( 6 of 10) ... skipped
Applying 148336-03 ( 7 of 10) ... skipped
Applying 146054-07 ( 8 of 10) ... skipped
Applying 142251-02 ( 9 of 10) ... skipped
Applying 125555-16 (10 of 10) ... skipped

Application of patches finished : 2017.10.26 20:48:08


Following patches were skipped :
 Patches already applied
 120900-04   119254-93   121296-01   148336-03   142251-02
 121133-02   119317-01   138215-03   146054-07   125555-16

Installation of prerequisite patches complete.

done
```

```
--apply-prereq  is given as argument so the sendmail config file is not backup and copy is not

Install log files written :
  /var/sadm/install_data/s10s_rec_patchset_short_2017.10.26_20.48.05.log
  /var/sadm/install_data/s10s_rec_patchset_verbose_2017.10.26_20.48.05.log

bash-3.2#
```

5.  Install the patchset into Alternate boot environment

```
#./installpatchset  –R /a
```

6.  Unmount and activate the altenate boot environemnt

```
# luumount /a
```

```
# luactivate  S10-Patches-2017-Q4
```

7.  Reboot the server

```
Backout instruction will be printed in the terminal
 # init 6
```

- **Note: If the server is configured with sendmail functionity, Please check sendmail functionality after patch the server both on Global and Non-Global Zones. Refer Known Issues section for more details.**

## 4.3 Solaris 10 - GSF Single-user install

**(Required)**

1.  Reboot system into a single-user runstate via:

```
 init 0
```

```
 boot –s (at the ok> prompt)
```

NOTE: Bringing a system down to a single-user runstate from a multi-user runstate via 'init s' may leave some services (such as automounted filesystems) in an inconsistent state not suitable for patching. Rebooting into single-user is the preferred method for entering a proper runstate for patch installation.

2.  Install the patchset

```
cd /var/tmp/S10-Patches-2017-Q4
```

```
./installpatchset
```

3.  Optionally, to validate patch installation (see Patch Validation below):

```
cd /var/tmp/S10-Patches-2017-Q4/soe/bart
```

```
./checkSignatures.sh
```

- **Note: If the server is configured with sendmail functionity, Please check sendmail functionality after patch the server both on Global and Non-Global Zones. Refer Known Issues section for more details.**

## 4.4 Patch Validation

Current Sun patching facilities do not provide for verification of patch installation or validation of patched files. To partially address this issue, PSE is providing manifests of MD5 signatures for patch target files along with a simple comparison tool. This tool should not be used as a guarantee of success, but rather used as an aid to help identify failures in patching.

To compare MD5 signatures and identify possible patch failures:

1. This may be done in any run-state (single-user or multi-user)

```
cd /var/tmp/S10-Patches-2017-Q4/soe/bart
```

  (Either local or NFS mount)

```
./checkSignatures.sh
```

The tool will generate both control (expected/correct) and test (actual/existing) manifests, compare them, and display discrepancies. Files listed should be manually verified to be correct.

Specific issues to note:

1. The listing of files not matching expected signatures does not necessarily indicate failure, and typical runs will generally identify at least one mismatch.

2. If newer revisions of patches that comprise this patchset are installed, some files in that patch will not match the expected MD5 signatures and will be identified by this tool. These may be ignored.

3. Kernel driver configuration files and system configuration files (in /etc) are explicitly ignored.

4. The time taken for the tool may vary based on CPU and I/O performance.


## 4.5 Patch Install Order

**\*Note that this patchset consist the patch list order below reflects the patch install order.**

120900-04  SunOS 5.10: libzonecfg Patch
121133-02  SunOS 5.10: zones library and zones utility patch
119254-93  SunOS 5.10: Install and Patch Utilities Patch
119317-01  SunOS 5.10: SVr4 Packaging Commands (usr) Patch
121296-01  SunOS 5.10: fgrep Patch
138215-03  SunOS 5.10: sort patch
148336-03  SunOS 5.10: awk patch
146054-07  Obsoleted by: 146696-04 SunOS 5.10: ksh patch
142251-02  SunOS 5.10: sh patch
125555-16  SunOS 5.10: patch behavior patch
118367-04  Obsoleted by: 118367-05 SunOS 5.10: csh Patch
118705-02  SunOS 5.10: XVR-1000 GFB Graphics Patch
118706-01  SunOS 5.10: Creator and Creator3D: FFB Graphics Patch
118707-05  SunOS 5.10: Expert3D IFB Graphics Patch
118708-19  Obsoleted by: 118708-20 SunOS 5.10: Sun XVR-1200 and Sun XVR-600 Graphics Accelerator Patch
118711-03  SunOS 5.10: M64 Graphics Patch
118712-23  Obsoleted by: 118712-24 SunOS 5.10: Sun XVR-100 Graphics Accelerator Patch
118718-06  Obsoleted by: 118718-07 SunOS 5.10: Generic Framebuffer configuration Graphics Patch
118777-18  Obsoleted by: 118777-19 SunOS 5.10: Sun GigaSwift Ethernet 1.0 driver patch
121181-05  Obsoleted by: 121181-06 Sun Trunking Utility 1.3: maintenance patch
118918-24  SunOS 5.10: Solaris Crypto Framework patch
138217-01  SunOS 5.10: svccfg & svcprop patch
119578-30  SunOS 5.10: FMA Patch
140860-02  SunOS 5.10: su patch
121453-02  SunOS 5.10: Sun Update Connection Client Foundation
121118-21  SunOS 5.10: Update Connection System Client 1.0.20
118833-36  SunOS 5.10: kernel patch
118945-01  SunOS 5.10: Sun Gigabit Ethernet 3.0 driver patch
118981-03  SunOS 5.10: Sun Quad FastEthernet qfe driver
119059-72  Obsoleted by: 119059-73 X11 6.6.2: Xsun patch

119063-02  SunOS 5.10: libXpm patch
119081-25  SunOS 5.10: CD-ROM Install Boot Image Patch
119115-35  Obsoleted by: 119115-36 Mozilla 1.7: patch
119117-52  Obsoleted by: 119117-53 Evolution 1.4.6 patch
119130-33  SunOS 5.10: Sun Fibre Channel Device Drivers
119213-33  NSS_NSPR_JSS 3.21: NSPR 4.11 / NSS 3.21 / JSS 4.3.2
119246-39  Obsoleted by: 119246-40 SunOS 5.10: Manual Page updates for Solaris 10
124628-10  Obsoleted by: 124628-11 SunOS 5.10: CD-ROM Install Boot Image Patch
119252-29  Obsoleted by: 119252-30 SunOS 5.10: System Administration Applications Patch
123611-05  X11 6.6.2: Trusted Extensions patch
119280-25  Obsoleted by: 119280-26 CDE 1.6: Runtime library patch for Solaris 10
119278-38  Obsoleted by: 119278-42 CDE 1.6: dtlogin patch
119282-01  CDE 1.6: GNOME/CDE Menu for Solaris 10
119309-03  SunOS 5.10: PGX32 Graphics
140899-01  SunOS 5.10: [ir].manifest patch
119313-42  SunOS 5.10: WBEM Patch
124188-03  SunOS 5.10: Trusted Solaris Attributes Patch
119315-19  Obsoleted by: 119315-20 SunOS 5.10: Solaris Management Applications Patch
120199-15  Obsoleted by: 120199-16 SunOS 5.10: sysidtool Patch
119534-29  Obsoleted by: 119534-30 SunOS 5.10: Flash Archive Patch
119538-19  Obsoleted by: 119538-20 GNOME 2.6.0: Window Manager Patch
120099-08  APOC 1.2: Sun Java(tm) Desktop System Configuration Shared Libraries
119546-08  APOC 1.2: APOC Configuration Agent Patch
119548-14  GNOME 2.6.0: Gnome Multi-protocol instant messaging client Patch
119648-03  SunOS 5.10: vlan driver patch
120272-40  SunOS 5.10: SMA patch
122640-05  SunOS 5.10: zfs genesis patch
126897-02  SunOS 5.10: Fault Manager Patch
127755-01  SunOS 5.10: Fault Manager patch
125503-02  SunOS 5.10: package-move-of-IP-objects patch
118731-01  Obsoleted by: 120011-14 SunOS 5.10: /usr/sbin/zonecfg patch
124204-04  Obsoleted by: 120473-05 SunOS 5.10: zfs patch
122660-10  Obsoleted by: 120011-14 SunOS 5.10: zones patch
125547-02  SunOS 5.10: zoneadm indirect dependency patch
140796-01  SunOS 5.10: umountall patch
120011-14  SunOS 5.10: kernel patch
139520-02  SunOS 5.10: package specific [ir].manifest removal patch
125891-01  SunOS 5.10: libc_psr_hwcap.so.1 patch
126540-02  SunOS 5.10: libumem library patch
127127-11  SunOS 5.10: kernel patch
138866-03  SunOS 5.10: sharetab patch
137137-09  SunOS 5.10: kernel patch
141016-01  SunOS 5.10: Dummy Patch
139555-08  SunOS 5.10: Kernel Patch
142292-01  SunOS 5.10: Place Holder patch
141444-09  SunOS 5.10: kernel patch
142911-01  SunOS 5.10: Place Holder patch
142933-05  SunOS 5.10: failsafe patch
142909-17  SunOS 5.10: kernel patch

144526-02  Obsoleted by: 144526-03 SunOS 5.10: place holder patch
144500-19  SunOS 5.10: Solaris kernel patch
147442-01  Obsoleted by: 147442-02 SunOS 5.10: place holder patch
147147-26  SunOS 5.10: kernel patch
150510-03  SunOS 5.10: /var/svc/manifest/system/sysidtool.xml patch
150551-03  SunOS 5.10: local-fs.xml patch
148071-19  SunOS 5.10: openssl patch
151912-09  SunOS 5.10: OpenSSL 1.0.2 patch
119757-42  SunOS 5.10: Samba patch
119764-07  Obsoleted by: 119764-08 SunOS 5.10: ipmitool patch
119783-40  SunOS 5.10: BIND patch
119810-08  SunOS 5.10: International Components for Unicode Patch
119812-22  X11 6.6.2: FreeType patch
119900-18  GNOME 2.6.0: GNOME libtiff - library for reading and writing TIFF Patch
119903-02  OpenWindows 3.7.3: Xview Patch
119906-22  GNOME 2.6.0: Virtual File System Framework patch
119955-05  Obsoleted by: 143733-03 CDE 1.6: Tooltalk Runtime patch for Solaris 10
119963-24  Obsoleted by: 119963-25 SunOS 5.10: Shared library patch for C++
119966-01  Obsoleted by: 119966-02 SunOS 5.10: Math Libraries (libm+libmvec) patch
119986-03  SunOS 5.10: clri patch
120094-36  X11 6.6.2: xscreensaver patch
120101-01  SunOS 5.10: libsmedia patch
120195-02  SunOS 5.10: patch schpc sc_gptwocfg gptwo_pci
120201-07  X11 6.8.0: Xorg client libraries patch
120256-01  SunOS 5.10: hci1394 Patch
120284-07  GNOME 2.6.0: GNOME CORBA ORB and component framework
120460-17  Obsoleted by: 120460-19 GNOME 2.6.0: Gnome libs Patch
119368-04  Obsoleted by: 119368-05 GNOME 2.6.0: Printing Technology Patch
120286-03  Obsoleted by: 120286-04 GNOME 2.6.0: Gnome text editor Patch
120292-02  Obsoleted by: 120292-03 SunOS 5.10: mysql patch
120348-03  Obsoleted by: 146234-01 SunOS 5.10: Fibre Channel HBA Port utility
121975-01  CDE 1.6: Xsession patch
120410-33  Obsoleted by: 120410-34 SunOS 5.10: Internet/Intranet Input Method Framework
patch
120412-11  Obsoleted by: 120412-12 SunOS 5.10: Simplified Chinese locale patch
120414-27  Obsoleted by: 120414-28 SunOS 5.10: Asian CCK locales patch
120543-36  Obsoleted by: 120543-37 SunOS 5.10: Apache 2 Patch
120719-07  SunOS 5.10: SunFreeware gzip patch
120732-01  SunOS 5.10: libusb patch
120739-08  GNOME 2.6.0: GNOME PDF Viewer based on Xpdf
120753-09  Obsoleted by: 120753-10 SunOS 5.10: Microtasking libraries (libmtsk) patch
120811-09  Obsoleted by: 120811-10 SunOS 5.10: FUJITSU PCI Fibre Channel Driver 3.0
patch
120812-32  OpenGL 1.5: OpenGL Patch for Solaris
120815-01  SunOS 5.10: dmfe patch
120830-06  SunOS 5.10: vi and ex patch
120849-04  SunOS 5.10: Sun PCI-E Gigabit Ethernet Adapter Patch
120928-32  Obsoleted by: 120928-33 SunOS 5.10: Sun XVR-2500 Graphics Accelerator Patch
121095-05  GNOME 2.6.0: GNOME EXIF tag parsing library for digital cameras

121104-11  SunOS 5.10: Adobe Acrobat Reader patch
121136-02  SunOS 5.10: Adobe Acrobat Reader browser-plugin patch
121211-02  SunOS 5.10: Sun Java Web Console (Lockhart) Patch
121308-20  Obsoleted by: 121308-21 SunOS 5.10: Solaris Management Console Patch
121337-01  SunOS 5.10: tlimod patch
120235-01  SunOS 5.10: Live Upgrade Zones Support Patch
121428-15  SunOS 5.10: Live Upgrade Zones Support Patch
121606-04  GNOME 2.6.0: Python patch
121946-01  SunOS 5.10: Error processing FRU tree: IO error patch
122031-01  SunOS 5.10: cgsix Patch
122212-46  GNOME 2.6.0: GNOME Desktop Patch
122259-09  SunOS 5.10: SunFreeware GNU ESP Ghostscript Patch
122470-03  Obsoleted by: 122470-04 GNOME 2.6.0: GNOME Java Help Patch
122472-07  SunOS 5.10: XVR200 Graphics
122911-37  SunOS 5.10: Apache 1.3 Patch
123003-04  SunOS 5.10: SAM module patch
124171-07  Obsoleted by: 124171-08 SunOS 5.10: SCN Base cacao module patch
123630-03  Obsoleted by: 123630-04 SunOS 5.10: HTTP proxy settings patch
123005-07  Obsoleted by: 123005-08 SunOS 5.10: Basic Registration Update
123252-01  SunOS 5.10: platform/SUNW,Netra-T2000 patch
123301-01  SunOS 5.10: i2c_svc patch
123358-02  SunOS 5.10: jumpstart and live upgrade compliance patch
123526-01  Obsoleted by: 148873-02 SunOS 5.10: libcurses patch
123590-12  SunOS 5.10: PostgresSQL patch
123893-79  Obsoleted by: 123893-80 SunOS 5.8 5.9 5.10: Common Agent Container (cacao)
runtime 2.4.7.0 upgrade patch 79
123938-05  GNOME 2.6.0: GNU Transport Layer Security Library Patch
124149-16  SunOS 5.10: Sun XVR-300 Graphics Accelerator Patch
124325-01  SunOS 5.10: rcm modules patch
124393-12  CDE 1.6: Dtlogin smf patch
124397-02  CDE 1.6: libDtWidget patch
124457-02  Obsoleted by: 124457-03 X11 6.6.2: xdm patch
124630-42  Obsoleted by: 124630-43 SunOS 5.10: System Administration Applications,
Network, and Core Libraries Patch
124939-05  SunOS 5.10 5.10_x86: JDMK 5.1 patch
124997-01  SunOS 5.10: /usr/bin/tip patch
125075-01  SunOS 5.10: svc-volfs patch
125215-07  SunOS 5.10: wget patch
125279-05  Obsoleted by: 125279-06 CDE 1.6: dtsession patch
125332-24  JDS 3: Macromedia Flash Player Plugin Patch
125505-01  SunOS 5.10: daktari and cherrystone header files patch
125533-17  Obsoleted by: 125533-18 GNOME 2.6.0: Trusted Extension Runtime Patch
125670-04  SunOS 5.10: Sun x8 10G/1G Ethernet Adapter driver patch
125719-58  X11 6.8.0: Xorg server patch
125725-03  X11 6.6.2: xinerama patch
125731-13  Obsoleted by: 125731-14 SunOS 5.10: XML and XSLT libraries patch
126119-02  CDE 1.6: sys-suspend patch
126206-12  SunOS 5.10: zebra ripd quagga patch
126363-10  SunOS 5.10: X Window System changes - Solaris Trusted Extensions

126365-16  Obsoleted by: 126365-17 SunOS 5.10: CDE Desktop changes - Solaris Trusted Extensions
126425-01  SunOS 5.10: fsckall patch
126440-01  Obsoleted by: 126440-02 SunOS 5.10: rm patch
126546-10  SunOS 5.10: bash patch
126630-06  SunOS 5.10: tcsh patch
126868-05  SunOS 5.10: SunFreeware bzip2 patch
127752-01  SunOS 5.10: SUNW,Netra-CP3060 platform symlinks patch
127872-02  SunOS 5.10: mailx patch
128292-01  SunOS 5.10: rsm Patch
128298-02  SunOS 5.10: se patch
128310-01  SunOS 5.10: hsfs patch
128332-01  SunOS 5.10: conskbd patch
136882-07  SunOS 5.10: ImageMagick patch
136893-02  SunOS 5.10: runacct patch
136998-10  SunOS 5.10: PostgreSQL 8.2 core patch
137000-08  SunOS 5.10: PostgreSQL 8.2 documentation patch
137004-09  SunOS 5.10: PostgreSQL 8.2 source code patch
137032-01  SunOS 5.10: namefs patch
137080-11  SunOS 5.10: libpng Patch
137090-02  SunOS 5.10: rmc_comm, rmclomv patch
137093-01  SunOS 5.10: logindevperm patch
137097-02  SunOS 5.10: inetd-upgrade patch
137102-01  SunOS 5.10: flowacct patch
137115-01  SunOS 5.10: SUNWcsr postinstall patch
137147-08  SunOS 5.10: libexpat patch
137282-01  SunOS 5.10: intpexec patch
137321-04  SunOS 5.10: p7zip patch
137871-02  SunOS 5.10: tk patch
138096-02  SunOS 5.10: syslogd patch
138181-01  SunOS 5.10: ike.preshared patch
138195-04  Service Tags 1.0: patch for Solaris 10
138245-01  SunOS 5.10: nss_compat patch
138247-01  Obsoleted by: 148381-02 SunOS 5.10: cdrw patch
138352-06  X11 6.6.2: fontconfig patch
138361-01  Obsoleted by: 138361-02 SunOS 5.10: snmpXdmid patch
138647-01  SunOS 5.10: /usr/bin/dircmp patch
138649-01  SunOS 5.10: i.renamenew r.renamenew patch
138766-01  SunOS 5.10: ldap-client manifest patch
138822-12  SunOS 5.10: PostgreSQL 8.3 documentation patch
138824-12  SunOS 5.10: PostgreSQL 8.3 source code patch
138826-12  SunOS 5.10: PostgreSQL 8.3 core patch
138852-01  SunOS 5.10: postreverse patch
138854-01  Obsoleted by: 146292-01 SunOS 5.10: sulogin patch
139099-04  Obsoleted by: 139099-05 SunOS 5.10: gtar patch
139289-02  SunOS 5.10: pgadmin3 patch
139291-02  SunOS 5.10: pgadmin3 sources patch
139615-01  SunOS 5.10: Foomatic patch
139620-01  Obsoleted by: 119278-42 CDE 1.6: Dthelp patch

139962-02  SunOS 5.10: i.rbac and patch postinstall patch
139980-01  SunOS 5.10: SunFire T200 libprtdiag_psr patch
139986-01  SunOS 5.10: rpc.ypupdated patch
140455-01  Obsoleted by: 140455-02 X11 6.6.2: VNC Viewer patch
140912-01  Obsoleted by: 140912-02 SunOS 5.10: ufsrestore patch
141032-01  SunOS 5.10: audit patch
141104-04  SunOS 5.10: ZFS Administration Java Web Console Patch
141496-01  SunOS 5.10: patchchk patch
141532-04  Obsoleted by: 146075-01 SunOS 5.10: in.mpathd patch
141548-01  SunOS 5.10: svccfg patch
141558-01  SunOS 5.10: acctcom patch
141586-01  Obsoleted by: 148985-01 SunOS 5.10: libgss.so.1 patch
142049-01  Obsoleted by: 149057-01 SunOS 5.10: llc2 patch
142234-01  Obsoleted by: 148029-01 SunOS 5.10: ntp.xml patch
142240-01  SunOS 5.10: ntpq patch
142244-02  SunOS 5.10: hme driver patch
142340-02  SunOS 5.10: libresolv.so.2 patch
142373-04  SunOS 5.10: AST Graphics Patch
142394-01  SunOS 5.10: icmp patch
142397-01  SunOS 5.10: libsasl.so.1 patch
142428-02  SunOS 5.10: unshare patch
142430-01  SunOS 5.10: libscf.so.1 patch
142529-01  SunOS 5.10: uptime w utmp_update whodo patch
142543-01  Obsoleted by: 142543-02 SunOS 5.10: svc-snmpdx libssagent.so.1 mibiisa snmpdx
snmpdx.xm patch
143139-02  SunOS 5.10: nfs_dlboot patch
143317-03  GNOME 2.6.0: Instant Messaging patch
143502-01  GNOME 2.6.0: Trusted Extensions patch
143506-12  GNOME 2.6.0: Python patch
143527-01  SunOS 5.10: mc-opl patch
143609-03  Obsoleted by: 143609-04 SunOS 5.10: svc-iscsitgt patch
143643-08  Obsoleted by: 147438-06 SunOS 5.10: libMPAPI.so libmpscsi_vhci.so
libMPAPI.so.1 libmpscsi_vhci.so.1 patch
143651-01  SunOS 5.10: hpc3130 patch
144664-01  SunOS 5.10: ntptrace patch
143725-11  SunOS 5.10: SunFreeware ntp patch
143731-01  SunOS 5.10: libaudiofile patch
143733-01  Obsoleted by: 143733-03 CDE 1.6: ToolTalk RPC patch
143739-01  SunOS 5.10: Gedit patch
143954-04  Obsoleted by: 149277-01 SunOS 5.10: mpxio-upgrade patch
144047-01  SunOS 5.10: traceroute patch
144106-01  Obsoleted by: 144180-02 SunOS 5.10: usr/lib/nfs/nfslogd patch
144188-02  SunOS 5.10: emlxs patch
144229-02  X11 6.6.2: libpixman patch
144325-01  Obsoleted by: 144325-02 SunOS 5.10: Resource Management User Interface
Patch
144327-02  SunOS 5.10: Solaris Product Registry Patch
144455-01  Obsoleted by: 143962-02 SunOS 5.10: audit_syslog.so.1 patch
144492-01  Obsoleted by: 144742-02 SunOS 5.10: JPool.jar patch

144569-01 Obsoleted by: 148223-02 SunOS 5.10: zonecfg patch
147002-01 SunOS 5.10: libxnet.so patch
144872-03 SunOS 5.10: ifconfig patch
144909-03 SunOS 5.10: yp method ldap patch
144911-02 Obsoleted by: 148237-01 SunOS 5.10: vold patch
144994-02 Obsoleted by: 144994-03 SunOS 5.10: Ant patch
144996-02 Obsoleted by: 144994-03 SunOS 5.10: Ant source patch
145006-09 SunOS 5.10: Webmin patch
145023-01 SunOS 5.10: rc scripts Solaris Containers patch
147217-05 SunOS 5.10: SUNWdbus-bindings-priv patch
145080-15 SunOS 5.10: Firefox patch
145096-03 Obsoleted by: 146586-03 SunOS 5.10: oce driver patch
145120-01 SunOS 5.10: auditd.xml patch
145200-13 Obsoleted by: 145200-14 SunOS 5.10: Thunderbird patch
145648-03 Obsoleted by: 145648-04 SunOS 5.10: qlge driver Patch
145929-05 Obsoleted by: 145929-06 SunOS 5.10: igb driver Patch
147143-17 SunOS 5.10: iSCSI patch
146288-03 SunOS 5.10: dcfs patch
146334-01 Obsoleted by: 146466-02 SunOS 5.10: zlogin patch
146582-05 Obsoleted by: 146582-06 SunOS 5.10: fmadm patch
146673-01 SunOS 5.10: auth_attr prof_attr patch
146679-01 SunOS 5.10: hxge patch
146681-02 Obsoleted by: 147799-03 SunOS 5.10: arp patch
146694-02 Obsoleted by: 146694-03 SunOS 5.10: cron patch
146834-02 Obsoleted by: 149217-02 SunOS 5.10: zones resource controls patch
146954-03 Obsoleted by: 146954-04 SunOS 5.10: routed patch
147023-01 SunOS 5.10: ds_snmp patch
147194-03 Obsoleted by: 148023-03 SunOS 5.10: bmc patch
147219-01 SunOS 5.10: libgphoto2.so.2.0.3 patch
147227-01 X11 6.6.2: xrdb patch
147272-01 SunOS 5.10: encrypt/decrypt patch
147378-01 Obsoleted by: 147378-02 SunOS 5.10: zip patch
147673-11 SunOS 5.10: Oracle Java Web Console 3.1 Patch
147793-22 SunOS 5.10: Kerberos patch
147797-04 Obsoleted by: 147797-05 SunOS 5.10: prstat patch
147805-01 Obsoleted by: 149061-02 SunOS 5.10: tl patch
147992-10 SunOS 5.10: Pidgin patch
148002-01 SunOS 5.10: libdbus-1.so.3.4.2 patch
148004-01 SunOS 5.10: libpixbufloader-gif.so patch
148006-01 SunOS 5.10: libogg patch
148027-03 Obsoleted by: 148027-04 SunOS 5.10: compress cp cpio ln mv pack pax tar patch
148031-05 SunOS 5.10: klmmod patch
148049-04 Obsoleted by: 148049-05 SunOS 5.10: pam_authtok_check patch
148104-23 Obsoleted by: 148104-24 SunOS 5.10: last, ssh/sshd patch
148112-02 SunOS 5.10: root_archive patch
148135-01 Obsoleted by: 149395-01 SunVTS 7.0: Patch Set 14 consolidation patch
148165-02 Obsoleted by: 148165-03 SunOS 5.10: password policy migration patch
148241-05 Obsoleted by: 148241-06 SunOS 5.10: statd patch
150312-06 Obsoleted by: 150312-07 SunOS 5.10: iscsi patch

148309-08  SunOS 5.10: dhcp patch
148322-13  Obsoleted by: 148322-14 SunOS 5.10: ixgbe patch
148342-09  Obsoleted by: 148342-10 SunOS 5.10: nxge patch
148383-01  SunOS 5.10: IPv6 patch
148403-01  SunOS 5.10: strmod/spppcomp patch
148407-01  Obsoleted by: 149171-02 SunOS 5.10: mount patch
148412-02  Obsoleted by: 148419-03 SunOS 5.10: nss_dns patch
148423-01  SunOS 5.10: /usr/ccs/bin/error patch
148559-18  SunOS 5.10: timezone patch
148561-12  SunOS 5.10: Perl patch
148565-01  SunOS 5.10: fdformat patch
148625-01  SunOS 5.10: in.tnamed patch
148627-02  SunOS 5.10: rmformat patch
148693-01  SunOS 5.10: pam_unix_cred patch
148768-02  SunOS 5.10: calendar diff3 spell uupick patch
148870-01  SunOS 5.10: mailx.rc patch
148881-03  SunOS 5.10: xntpd patch
150435-04  SunOS 5.10: place holder patch
148888-05  SunOS 5.10: kernel patch
148948-01  SunOS 5.10: bsmconv bsmunconv patch
148975-01  SunOS 5.10: in.rexecd patch
149067-01  SunOS 5.10: SunFreeware GNU grep
149071-01  SunOS 5.10: Texinfo patch
149075-01  SunOS 5.10: pstools patch
149108-01  SunOS 5.10: libgsf-1.so.1.8.2 patch
149112-01  Obsoleted by: 149112-02 SunOS 5.10: libglib-2.0.so.0.1800.3 patch
149149-01  SunOS 5.10: LP Alerts Patch
149163-01  SunOS 5.10: rlmod patch
149165-01  SunOS 5.10: timod patch
150400-55  Obsoleted by: 150400-56 SunOS 5.10: Kernel Patch
149167-06  Obsoleted by: 149167-07 SunOS 5.10: qlcnic patch
149173-07  Obsoleted by: 149173-08 SunOS 5.10: emlxs driver patch
149175-10  Obsoleted by: 149175-11 SunOS 5.10: qlc patch
149279-04  SunOS 5.10: fabric-xlate.so PCIEX.dict patch
149312-04  SunOS 5.10: snoop patch
121081-08  SunOS 5.10: Connected Customer Agents 1.1.0
149453-02  SunOS 5.10: CCR Update
149483-01  SunOS 5.10: Foomatic patch
149496-02  SunOS 5.10: pppd patch
149638-05  SunOS 5.10: USB patch
149646-02  Obsoleted by: 149646-03 SunOS 5.10: nscd patch
150025-01  SunOS 5.10: pciexrc.eft patch
150031-15  Obsoleted by: 150031-16 SunOS 5.10: vsw patch
150032-01  SunOS 5.10: pcieb patch
150107-03  SunOS 5.10: ds patch
150113-02  Obsoleted by: 150113-03 SunOS 5.10: sockfs patch
150119-04  SunOS 5.10: kssl patch
150123-01  Obsoleted by: 150123-02 SunOS 5.10: sharefs patch
150157-01  SunOS 5.10: RPC patch

150173-01  Obsoleted by: 150173-02 SunOS 5.10: printer patch
150180-02  SunOS 5.10: sun4vpi.so patch
150310-02  Obsoleted by: 150310-03 SunOS 5.10: libc_psr_hwcap4.so.1 patch
150383-19  SunOS 5.10: wanboot patch
150534-01  SunOS 5.10: zoneadmd patch
150535-01  SunOS 5.10: libtopo.so.1 patch
150537-01  SunOS 5.10: event-transport.so patch
150539-01  SunOS 5.10: ip-transport.so patch
150545-02  SunOS 5.10: pam_ldap.so.1 patch
150616-01  SunOS 5.10: Evince Patch
150618-02  Obsoleted by: 150618-03 SunOS 5.10: OCM Patch
150631-04  SunOS 5.10: ehci patch
150832-12  Obsoleted by: 150832-13 SunOS 5.10: ufs patch
150836-01  Obsoleted by: 150836-02 SunOS 5.10: keyserv patch
150912-01  SunOS 5.10: pci_pci patch
151074-06  SunOS 5.10: sendmail patch
151148-01  SunOS 5.10: libadm.so.1 patch
151355-01  SunOS 5.10: cpc patch
151561-01  SunOS 5.10: libshare_nfs.so.1 patch
151615-01  Obsoleted by: 151615-02 SunOS 5.10: fcp patch
151696-01  SunOS 5.10: drctl patch
151717-01  SunOS 5.10: zsh patch
151719-01  SunOS 5.10: zsh source patch
151721-01  GNOME 2.6.0: GDK-PixBuf library Patch
151723-01  GNOME 2.6.0: word-list-compress Patch
151755-02  SunOS 5.10: libkmsagent.so.1 patch
151914-07  SunOS 5.10: OpenSSL 0.9.7 patch
152076-71  JavaSE 6: update 171 patch (equivalent to JDK 6u171)
152077-71  JavaSE 6: update 171 patch (equivalent to JDK 6u171), 64bit
152083-01  SunOS 5.10: wscons patch
152096-61  JavaSE 7: update 161 patch (equivalent to JDK 7u161)
152097-61  JavaSE 7: update 161 patch (equivalent to JDK 7u161), 64bit
152100-52  JavaSE 8: update 152 patch (equivalent to JDK 8u152), 64bit
152248-01  SunOS 5.10: rsync Patch
152250-01  SunOS 5.10: rsync Source Patch
150121-01  Obsoleted by: 150121-02 SunOS 5.10: audit_event patch
152252-02  SunOS 5.10: sudo Patch
152260-03  SunOS 5.10: libnsl patch
152264-01  SunOS 5.10: rpcbind patch
152363-01  SunOS 5.10: tem patch
152506-01  SunOS 5.10: elfexec patch
152510-06  SunOS 5.10: Tomcat 8 patch
152514-02  SunOS 5.10: Tomcat 6 Patch
152643-05  SunOS 5.10: Apache 2.4 Patch
152647-01  SunOS 5.10: nfsmapid patch
152649-02  CDE 1.6: dtappgather patch
152651-01  GNOME 2.6.0: libgdk-x11-2.0.so patch
152724-01  GNOME 2.6.0: libgdk-pixbuf-2.0.so patch
152728-01  SunOS 5.10: /platform/sun4v/kernel/cpu/sparcv9/SPARC-3e40 patch

149173-09  : SunOS 5.10: emlxs/fp driver patch

Extra Patches:
The patchset contains the following patches which are themselves obsoleted by
other patches in the patchset. These patches are required to ensure correct
installation of the patchset on Solaris 10 11/06 (Update 3) and earlier Solaris
10 Updates. The obsolete patches will only be applied to those systems where
they are necessary, they will not be applied if the system is already at a
higher patch level.

Patch      Reason
122660-10: Obsolete patch required by 125547-02. 125547-02 is the zoneadm
           indirect dependency patch, which is needed to resolve an issue
           applying kernel patch 120011-14 on a system with zones support. See
           CR 6471974.
124204-04: Obsolete patch required by 122660-10.
118731-01: Obsolete patch required by 124204-04.

The patchset contains the following patches for Unbundled Software Products (ie.
add on products that are not part of a default Solaris 10 installation). Patches
for Unbundled Products are included in the patchset only if their use is
required to avoid critical OS problems. These patches will only be applied to
systems where the associated Unbundled Product is installed.

Patch      Reason
121181-05: Patch is required to avoid a kernel panic caused by an
           incompatibility between Sun Trunking Utility and GigaSwift Ethernet
           drivers (see MOS article 1000555.1).
Live Upgrade patch 121430-XX is included in the patches/ directory of the
patchset, but this patch will not be applied during patchset installation. The
decision to apply the Live Upgrade patch is left to the user, this is done to
accommodate users who wish to independently manage the version of the Live
Upgrade patch on their system. Where a user wishes to apply the Live Upgrade
patch, this needs to be done manually with the patchadd command.

Patches for removed products:
Certain products that are components of earlier Solaris 10 Updates were removed
from Solaris 10 as it evolved. Patches for removed products are not relevant to
later solaris 10 Updates, and therefore have been excluded from this patchset.
The excluded patches are listed below, to allow a user to determine if any are
applicable to products that may still be installed on their systems.

Patch      Product
120185     StarOffice 8
125541-06  Mozilla 1.7 Thunderbird email client
125539-06  Mozilla 1.7 Firefox Web browser
122958-06  RealPlayer media application

# 5 KNOWN ISSUES

- This Patchset updates the /etc/mail/sendmail.cf file and the patch process will create backup of the original file with an .old extension in /etc/mail/ directory .This patchset restored the sendmail configuration files automatically however due to some reason if not restored properly the file /etc/mail/sendmail.cf.old  will need to be copied back as /etc/mail/sendmail.cf  to restore sendmail functionality. Restart the service if you are restore the file after reboot.

- If the server configured with sendmail functionality , do check the sendmail functionity after patch the server both on Global and Non-Global Zones. If sendmail not working properly do below steps manually

  Restore the  /etc/mail/sendmail.cf.old  to /etc/mail/sendmail.cf using copy command

  > mv /etc/mail/sendmail.cf /etc/mail/sendmail.cf_Q4-17
  > mv /etc/mail/submit.cf /etc/mail/submit.cf_Q4-17
  > cp –rfp  /etc/mail/sendmail.cf.old   /etc/mail/sendmail.cf
  > cp –rfp /etc/mail/submit.cf.old /etc/mail/submit.cf

- Patch 150551-03 will be canceled due to prepatch termination while Live upgrade insatallation method and this patch ONLY provides supporting functionality for zone root filesystems on iSCSI backed storage.

- If the non-global the zones will not in  HALT  (installed state)  we will get below error message and the patch update will abort

  ```
  "Native non-global zones need to be in the halted state before
  installing"
  ```

- Incldued the patch 149173-09  in this patch bundle to update the emlxs/fp driver, Recommended by Oracle for solution for PCI driver becomes unresponsive

# 6 BACK OUT PLANS

To back out a BAU patch set you must use Live Upgrade or split the root mirror prior to installation. It is impossible to back out a BAU patch set that is applied to a live system.

# 7 APPENDIX

## 7.1 VTM ID addressed on Solaris 10 - VTM Solutions - 2017Q4-1

| VTM ID | CVE ID | CVE description | Due Date | Package Name | Patch Number | Superseding Patch Information |
|--------|--------|-----------------|----------|--------------|--------------|-------------------------------|
| 79135 | CVE-2017-10388 | Oracle Java SE CVE-2017-10388 Remote Security Vulnerability | January 15, 2018 | SUNWj6dmo, SUNWj6dev, SUNWj6man, SUNWj6rt, SUNWj6cfg | 152076-71 | Not Applicable (Latest package |
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-71 | |
| 79150 | CVE-2017-10346 | Oracle Java SE CVE-2017-10346 Remote Security Vulnerability | January 15, 2018 | SUNWj6dmo, SUNWj6dev, SUNWj6man, SUNWj6rt, SUNWj6cfg | 152076-71 | Not Applicable (Latest package |
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-71 | |
| 79165 | CVE-2017-10285 | Oracle Java SE CVE-2017-10285 Remote Security Vulnerability | January 15, 2018 | SUNWj6dmo, SUNWj6dev, SUNWj6man, SUNWj6rt, SUNWj6cfg | 152076-71 | Not Applicable (Latest package |
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-71 | |
| 79180 | CVE-2017-10274 | Oracle Java SE CVE-2017-10274 Remote Security Vulnerability | January 15, 2018 | SUNWj6dmo, SUNWj6dev, SUNWj6man, SUNWj6rt, SUNWj6cfg | 152076-71 | Not Applicable (Latest package |
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-71 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 79212 | CVE-2017-10357 | Oracle Java SE CVE-2017-10357 Remote Security Vulnerability | May 3, 2018 | SUNWj6dmo, SUNWj6dev, SUNWj6man, SUNWj6rt, SUNWj6cfg | 152076-71 | Not Applicable (Latest package |
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-71 | |
| 79237 | CVE-2017-10349 | Oracle Java SE CVE-2017-10349 Remote Security Vulnerability | May 3, 2018 | SUNWj6dmo, SUNWj6dev, SUNWj6man, SUNWj6rt, SUNWj6cfg | 152076-71 | Not Applicable (Latest package |
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-71 | |
| 79252 | CVE-2017-10348 | Oracle Java SE CVE-2017-10348 Remote Security Vulnerability | May 3, 2018 | SUNWj6dmo, SUNWj6dev, SUNWj6man, SUNWj6rt, SUNWj6cfg | 152076-71 | Not Applicable (Latest package |
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-71 | |
| 79275 | CVE-2017-10293 | Oracle Java SE CVE-2017-10293 Remote Security Vulnerability | May 3, 2018 | SUNWj6dmo, SUNWj6dev, SUNWj6man, SUNWj6rt, SUNWj6cfg | 152076-71 | Not Applicable (Latest package |
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-71 | |
| 79305 | CVE-2017-10355 | Oracle Java SE and JRockit CVE-2017-10355 Remote Security Vulnerability | May 3, 2018 | SUNWj6dmo, SUNWj6dev, SUNWj6man, SUNWj6rt, SUNWj6cfg | 152076-71 | Not Applicable (Latest package |
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-71 | |

| 79329 | CVE-2017-10347 | Oracle Java SE and JRockit CVE-2017-10347 Remote Security Vulnerability | May 3, 2018 | SUNWj6dmo, SUNWj6dev, SUNWj6man, SUNWj6rt, SUNWj6cfg | 152076-71 | Not Applicable (Latest package |
| --- | --- | --- | --- | --- | --- | --- |
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-71 | |
| 79374 | CVE-2017-10281 | Oracle Java SE and JRockit CVE-2017-10281 Remote Security Vulnerability | May 3, 2018 | SUNWj6dmo, SUNWj6dev, SUNWj6man, SUNWj6rt, SUNWj6cfg | 152076-71 | Not Applicable (Latest package |
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-71 | |
| 79413 | CVE-2016-10165 | lcms2 CVE-2016-10165 Out-of-Bounds Read Denial of Service Vulnerability | May 3, 2018 | SUNWj6dmo, SUNWj6dev, SUNWj6man, SUNWj6rt, SUNWj6cfg | 152076-71 | Not Applicable (Latest package |
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-71 | |
| 75004 | CVE-2017-3629 | Oracle Solaris CVE-2017-3629 Local Privilege Escalation Vulnerability | July 1, 2018 | SUNWrcmds SUNWhea SUNWgss SUNWgssk SUNWrcmdc SUNWkdcu SUNWkrbu SUNWtnetd SUNWtnetc | 147793-22 | Not Applicable (Latest package |
| | | | | SUNWarc SUNWzfsu SUNWcry SUNWcakr SUNWftdur SUNWhermon SUNWnfscr SUNWust1 SUNWintgige SUNWnfssu SUNWpd SUNWmdb SUNWcar SUNWpdu SUNWnfsskr | 150400-55 | |

| VTM ID | CVE ID | CVE description | Due Date | Package Name | Patch Number | Superseding Patch Information |
|---|---|---|---|---|---|---|
| | | | | SUNWmptsas SUNWpkcs11 kms SUNWsmapi SUNWnfscu | | |
| 71266 | CVE-2017-6463 | NTP CVE-2017-6462 Denial of Service Vulnerability | February 19, 2018 | SUNWntp4u, SUNWntp4r | 143725-11 | Not Applicable (Latest package |
| 71266 | CVE-2017-6463 | NTP CVE-2017-6463 Denial of Service Vulnerability | February 19, 2018 | SUNWntp4u, SUNWntp4r | 143725-11 | Not Applicable (Latest package |
| 71260 | CVE-2017-6464 | NTP CVE-2017-6464 Denial of Service Vulnerability | December 5, 2017 | SUNWntp4u, SUNWntp4r | 143725-11 | Not Applicable (Latest package |

# 7.2 VTM ID addressed on Solaris 10 - VTM Solutions - 2017Q3-1

| VTM ID | CVE ID | CVE description | Due Date | Package Name | Patch Number | Superseding Patch Information |
|---|---|---|---|---|---|---|
| 75824 | CVE-2017-10110 | Oracle Java SE CVE-2017-10110 Remote Security Vulnerability | October 15, 2017 | SUNWj6dmo, SUNWj6dev, SUNWj6man, SUNWj6rt, SUNWj6cfg | 152076-61 | 152076-61 and above &152077-61 and above |
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-61 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 75839 | CVE-2017-10089 | Oracle Java SE CVE-2017-10089 Remote Security Vulnerability | October 15, 2017 | SUNWj6dmo, SUNWj6dev, SUNWj6man, SUNWj6rt, SUNWj6cfg | 152076-61 | 152076-61 and above &152077-61 and above |
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-61 | |
| 75878 | CVE-2017-10074 | Oracle Java SE CVE-2017-10074 Remote Security Vulnerability | October 16, 2017 | SUNWj6dmo, SUNWj6dev, SUNWj6man, SUNWj6rt, SUNWj6cfg | 152076-61 | 152076-61 and above &152077-61 and above |
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-61 | |
| 75893 | CVE-2017-10116 | Oracle Java SE and JRockit CVE-2017-10116 Remote Security Vulnerability | October 16, 2017 | SUNWj6dmo, SUNWj6dev, SUNWj6man, SUNWj6rt, SUNWj6cfg | 152076-61 | 152076-61 and above &152077-61 and above |
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-61 | |
| 75915 | CVE-2017-10067 | Oracle Java SE CVE-2017-10067 Remote Security Vulnerability | October 16, 2017 | SUNWj6dmo, SUNWj6dev, SUNWj6man, SUNWj6rt, SUNWj6cfg | 152076-61 | 152076-61 and above &152077-61 and above |
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-61 | |
| 75930 | CVE-2017-10096 | Oracle Java SE CVE-2017-10096 Remote Security Vulnerability | October 16, 2017 | SUNWj6dmo, SUNWj6dev, SUNWj6man, SUNWj6rt, SUNWj6cfg | 152076-61 | 152076-61 and above &152077-61 and above |
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-61 | |

| 75945 | CVE-2017-10101 | Oracle Java SE CVE-2017-10101 Remote Security Vulnerability | October 16, 2017 | SUNWj6dmo, SUNWj6dev, SUNWj6man, SUNWj6rt, SUNWj6cfg | 152076-61 | 152076-61 and above &152077-61 and above |
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-61 | |
| 75964 | CVE-2017-10087 | Oracle Java SE CVE-2017-10087 Remote Security Vulnerability | October 16, 2017 | SUNWj6dmo, SUNWj6dev, SUNWj6man, SUNWj6rt, SUNWj6cfg | 152076-61 | 152076-61 and above &152077-61 and above |
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-61 | |
| 76062 | CVE-2017-10107 | Oracle Java SE CVE-2017-10107 Remote Security Vulnerability | October 16, 2017 | SUNWj6dmo, SUNWj6dev, SUNWj6man, SUNWj6rt, SUNWj6cfg | 152076-61 | 152076-61 and above &152077-61 and above |
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-61 | |
| 75976 | CVE-2017-10176 | Oracle Java SE and JRockit CVE-2017-10176 Remote Security Vulnerability | October 16, 2017 | SUNWj6dmo, SUNWj6dev, SUNWj6man, SUNWj6rt, SUNWj6cfg | 152076-61 | 152076-61 and above &152077-61 and above |
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-61 | |
| 75995 | CVE-2017-10118 | Oracle Java SE and JRockit CVE-2017-10118 Remote Security Vulnerability | October 16, 2017 | SUNWj6dmo, SUNWj6dev, SUNWj6man, SUNWj6rt, SUNWj6cfg | 152076-61 | 152076-61 and above &152077-61 and above |
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-61 | |

| 76021 | CVE-2017-10115 | Oracle Java SE and JRockit CVE-2017-10115 Remote Security Vulnerability | October 16, 2017 | SUNWj6dmo, SUNWj6dev, SUNWj6man, SUNWj6rt, SUNWj6cfg | 152076-61 | 152076-61 and above &152077-61 and above |
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-61 | |
| 76052 | CVE-2017-10102 | Oracle Java SE CVE-2017-10102 Remote Security Vulnerability | February 1, 2018 | SUNWj6dmo, SUNWj6dev, SUNWj6man, SUNWj6rt, SUNWj6cfg | 152076-61 | 152076-61 and above &152077-61 and above |
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-61 | |
| 76138 | CVE-2017-10042 | Oracle Solaris CVE-2017-10042 Remote Security Vulnerability | October 16, 2017 | SUNWarc SUNWzfsu SUNWcry SUNWcakr SUNWftdur SUNWhermon SUNWnfscr SUNWust1 SUNWintgige SUNWnfssu SUNWpd SUNWmdb SUNWcar SUNWpdu SUNWnfsskr SUNWmptsas SUNWpkcs11kms SUNWsmapi SUNWnfscu | 150400-52 | 150400-52 and above |

| 76141 | CVE-2017-10036 | Oracle Solaris CVE-2017-10036 Remote Security Vulnerability | October 16, 2017 | SUNWarc<br>SUNWzfsu<br>SUNWcry<br>SUNWcakr<br>SUNWftdur<br>SUNWhermon<br>SUNWnfscr<br>SUNWust1<br>SUNWintgige<br>SUNWnfssu<br>SUNWpd<br>SUNWmdb<br>SUNWcar<br>SUNWpdu<br>SUNWnfsskr<br>SUNWmptsas<br>SUNWpkcs11kms<br>SUNWsmapi<br>SUNWnfscu | 150400-52 | 150400-52 and above |
|---|---|---|---|---|---|---|
| 76144 | CVE-2017-10004 | Oracle Solaris CVE-2017-10004 Local Security Vulnerability | February 1, 2018 | SUNWarc<br>SUNWzfsu<br>SUNWcry<br>SUNWcakr<br>SUNWftdur<br>SUNWhermon<br>SUNWnfscr<br>SUNWust1<br>SUNWintgige<br>SUNWnfssu<br>SUNWpd<br>SUNWmdb<br>SUNWcar<br>SUNWpdu<br>SUNWnfsskr<br>SUNWmptsas<br>SUNWpkcs11kms<br>SUNWsmapi<br>SUNWnfscu | 150400-52 | 150400-52 and above |
| 76156 | CVE-2017-10243 | Oracle Java SE and JRockit CVE-2017-10243 Remote Security Vulnerability | February 1, 2018 | SUNWj6dmo,<br>SUNWj6dev,<br>SUNWj6man,<br>SUNWj6rt,<br>SUNWj6cfg | 152076-61 | 152076-61 and above &152077-61 and above |

| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-61 | |
|---|---|---|---|---|---|---|
| 76171 | CVE-2017-10198 | Oracle Java SE and JRockit CVE-2017-10198 Remote Security Vulnerability | February 1, 2018 | SUNWj6dmo, SUNWj6dev, SUNWj6man, SUNWj6rt, SUNWj6cfg | 152076-61 | 152076-61 and above &152077-61 and above |
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-61 | |
| 76186 | CVE-2017-10135 | Oracle Java SE and JRockit CVE-2017-10135 Remote Security Vulnerability | February 1, 2018 | SUNWj6dmo, SUNWj6dev, SUNWj6man, SUNWj6rt, SUNWj6cfg | 152076-61 | 152076-61 and above &152077-61 and above |
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-61 | |
| 76202 | CVE-2017-10053 | Oracle Java SE and JRockit CVE-2017-10053 Remote Security Vulnerability | February 1, 2018 | SUNWj6dmo, SUNWj6dev, SUNWj6man, SUNWj6rt, SUNWj6cfg | 152076-61 | 152076-61 and above &152077-61 and above |
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-61 | |
| 76244 | CVE-2017-10108 | Oracle Java SE and JRockit CVE-2017-10108 Remote Security Vulnerability | February 1, 2018 | SUNWj6dmo, SUNWj6dev, SUNWj6man, SUNWj6rt, SUNWj6cfg | 152076-61 | 152076-61 and above &152077-61 and above |
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-61 | |
| 76262 | CVE-2017-10109 | Oracle Java SE and JRockit CVE-2017-10109 Remote Security Vulnerability | February 1, 2018 | SUNWj6dmo, SUNWj6dev, SUNWj6man, SUNWj6rt, SUNWj6cfg | 152076-61 | 152076-61 and above &152077-61 and above |
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-61 | |

| 75856 | CVE-2017-3632 | Oracle Solaris CVE-2017-3632 Remote Security Vulnerability | October 16, 2017 | SUNWdtbas SUNWdtdmr | 124393-12 | Not Applicable (Latest package) |

## 7.3 VTM ID addressed on Solaris 10 - VTM Solutions - 2017Q2-1

| VTM ID | CVE ID | CVE description | Due Date | Package Name | Patch Number | Superseding Patch Information |
|---|---|---|---|---|---|---|
| 72083 | CVE-2017-3623 | Oracle Solaris CVE-2017-3623 Remote Security Vulnerability | July,17 2017 | SUNWcakr.v SUNWhea FJSVmdbr SUNWckr SUNWintgige SUNWcsr SUNWiopc.v SUNWcsu SUNWldomr.v SUNWdtrc SUNWldomu.v SUNWarc SUNWefc.u SUNWmdb SUNWcakr.u SUNWefc.us SUNWmdbr SUNWcakr.us SUNWefcl SUNWperl584core | 150400-02, 148888-05 and 147147-26 | 147440-10 and above or 147147-26 or 148888-01 and above 150400-01 and above |
| 72095 | CVE-2017-3514 | Oracle Java SE CVE-2017-3514 Remote Security Vulnerability | July,17 2017 | SUNWj6dmo SUNWj6dev SUNWj6man SUNWj6rt SUNWj6cfg | 152076-51 | 152076-51 and above &152077-51 and above |

| VTM ID | CVE ID | CVE description | Due Date | Package Name | Patch Number | Superseding Patch Information |
|---|---|---|---|---|---|---|
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-51 | |
| 68067 | CVE-2016-9311 | NTP CVE-2016-9311 NULL Pointer Dereference Denial of Service Vulnerability | November,19 2017 | SUNWntp4u, SUNWntp4r | 143725-10 | 143725-10 and above |
| 68074 | CVE-2016-9310 | NTP CVE-2016-9310 Denial of Service Vulnerability | November,19 2017 | SUNWntp4u, SUNWntp4r | 143725-10 | 143725-10 and above |
| 68092 | CVE-2016-7431 | NTP CVE-2016-7431 Denial of Service Vulnerability | November,19 2017 | SUNWntp4u, SUNWntp4r | 143725-10 | 143725-10 and above |
| 68104 | CVE-2016-7428 | NTP CVE-2016-7428 Denial of Service Vulnerability | November,19 2017 | SUNWntp4u, SUNWntp4r | 143725-10 | 143725-10 and above |
| 68110 | CVE-2016-7427 | NTP CVE-2016-7427 Denial of Service Vulnerability | November,19 2017 | SUNWntp4u, SUNWntp4r | 143725-10 | 143725-10 and above |
| 72110 | CVE-2017-3509 | Oracle Java SE CVE-2017-3509 Remote Security Vulnerability | November, 2 2017 | SUNWj6dmo SUNWj6dev SUNWj6man SUNWj6rt SUNWj6cfg | 152076-51 | 152076-51 and above &152077-51 and above |
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-51 | |
| 72165 | CVE-2017-3526 | Oracle Java SE and JRockit CVE-2017-3526 Remote Security Vulnerability | November, 2 2017 | SUNWj6dmo SUNWj6dev SUNWj6man SUNWj6rt SUNWj6cfg | 152076-51 | 152076-51 and above &152077-51 and above |
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-51 | |

## 7.4 VTM ID addressed on Solaris 10 - VTM Solutions - 2017Q1-1

| VTM ID | CVE ID | CVE description | Due Date | Package Name | Patch Number | Superseding Patch Information |
|--------|--------|-----------------|----------|--------------|--------------|-------------------------------|
| 67051 | CVE-2017-2335 | 7-Zip Multiple Remote Code Execution Vulnerabilities | August 4, 2017 | SUNWbzip | 137321-04 | Not Applicable (Latest package) |
| 69325 | CVE-2017-3272 | Oracle Java SE CVE-2017-3272 Remote Security Vulnerability | April 17, 2017 | SUNWj6dmo SUNWj6dev SUNWj6man SUNWj6rt SUNWj6cfg | 152076-41 | 152076-41 and above &152077-41 and above |
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-41 | |
| 69415 | CVE-2016-5548 | Oracle Java SE CVE-2016-5548 Remote Security Vulnerability | August 3, 2017 | SUNWj6dmo SUNWj6dev SUNWj6man SUNWj6rt SUNWj6cfg | 152076-41 & | 152076-41 and above &152077-41 and above |
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-41 | |
| 69429 | CVE-2017-3253 | Oracle Java SE and JRockit CVE-2017-3253 Remote Security Vulnerability | April 17, 2017 | SUNWj6dmo SUNWj6dev SUNWj6man SUNWj6rt SUNWj6cfg | 152076-41 | 152076-41 and above &152077-41 and above |
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-41 | |

| VTM ID | CVE ID | CVE description | Due Date | Package Name | Patch Number | Superseding Patch Information |
|---|---|---|---|---|---|---|
| 69443 | CVE-2017-3252 | Oracle Java SE and JRockit CVE-2017-3252 Remote Security Vulnerability | August 3, 2017 | SUNWj6dmo SUNWj6dev SUNWj6man SUNWj6rt SUNWj6cfg | 152076-41 | 152076-41 and above &152077-41 and above |
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-41 | |
| 69457 | CVE-2017-3241 | Oracle Java SE and JRockit CVE-2017-3241 Remote Security Vulnerability | August 3, 2017 | SUNWj6dmo SUNWj6dev SUNWj6man SUNWj6rt SUNWj6cfg | 152076-41 | 152076-41 and above &152077-41 and above |
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-41 | |
| 69472 | CVE-2016-5552 | Oracle Java SE and JRockit CVE-2016-5552 Remote Security Vulnerability | August 3, 2017 | SUNWj6dmo SUNWj6dev SUNWj6man SUNWj6rt SUNWj6cfg | 152076-41 | 152076-41 and above &152077-41 and above |
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-41 | |
| 69495 | CVE-2016-5546 | Oracle Java SE and JRockit CVE-2016-5546 Remote Security Vulnerability | April 17, 2017 | SUNWj6dmo SUNWj6dev SUNWj6man SUNWj6rt SUNWj6cfg | 152076-41 | 152076-41 and above &152077-41 and above |
| | | | | SUNWj6dmx SUNWj6rtx SUNWj6dvx | 152077-41 | |

## 7.5 VTM ID addressed on Solaris 10 - VTM Solutions - 2016Q4-1

| VTM ID | CVE ID | CVE description | Due Date | Package information | Patch Number | Superseding Patch Information |
|---|---|---|---|---|---|---|
| 59822 | CVE-2015-8138 | [BID-81811] NTP CVE-2015-8138 Denial of Service Vulnerability | June 6, 2017 | SUNWntp4u | 143725-09 | 143725-09 and above |
| 59827 | CVE-2015-7979 | [BID-81816] NTP CVE-2015-7979 Denial of Service Vulnerability | August 11, 2016 | SUNWntp4u | 143725-09 | 143725-09 and above |
| 59896 | CVE-2015-8140 | [BID-82102] NTP CVE-2015-8140 Security Bypass Vulnerability | August 13, 2016 | SUNWntp4u | 143725-09 | 143725-09 and above |
| 59901 | CVE-2015-8139 | [BID-82105] NTP CVE-2015-8139 Security Bypass Vulnerability | August 13, 2016 | SUNWntp4u | 143725-09 | 143725-09 and above |
| 60229 | CVE-2014-9298 | RETIRED: Network Time Protocol CVE-2014-9298 Authentication Bypass Vulnerability | August 27, 2016 | SUNWntp4u | 143725-09 | 143725-09 and above |
| 60479 | CVE-2010-2252 | GNU Wget CVE-2010-2252 Arbitrary File Overwrite Vulnerability | June 6, 2017 | SUNWwgetr | 125215-07 | 125215-07 and above |
| 61563 | CVE-2016-1286 | ISC BIND CVE-2016-1286 Remote Denial of Service Vulnerability | March 22, 2017 | SUNWbindr | 119783-37 | 119783-37 and above |
| 61567 | CVE-2016-1285 | ISC BIND CVE-2016-1285 Remote Denial of Service Vulnerability | March 22, 2017 | SUNWbindr | 119783-37 | 119783-37 and above |

| VTM ID | CVE ID | CVE description | Due Date | Package information | Patch Number | Superseding Patch Information |
|---|---|---|---|---|---|---|
| 61579 | CVE-2016-0800 | OpenSSL DROWN Attack CVE-2016-0800 Security Bypass Vulnerability | June 6, 2017 | SUNWwbsup | 150383-16 | 150383-16 and above |
| 61594 | CVE-2015-3197 | OpenSSL CVE-2015-3197 Security Bypass Vulnerability | June 6, 2017 | SUNWopenssl-include | 151914-07 | 151914-07 and above |
| 62098 | CVE-2016-0693 | Oracle Solaris CVE-2016-0693 Remote Security Vulnerability | March 22, 2017 | SUNWcsl | 150545-02 | 150545-02 and above |
| 62201 | CVE-2016-3441 | Oracle Solaris CVE-2016-3441 Local Security Vulnerability | June 6, 2017 | SUNWnfsskr | 150400-40 | 150400-40 and above |
| 62251 | CVE-2015-7236 | rpcbind 'rpcb_svc_com.c' Remote Memory Corruption Vulnerability | June 6, 2017 | SUNWcsu | 152264-01 | 152264-01 and above |
| 62424 | CVE-2016-2516 | NTP CVE-2016-2516 Denial of Service Vulnerability | June 6, 2017 | SUNWntp4u | 143725-09 | 143725-09 and above |
| 62469 | CVE-2016-1548 | NTP CVE-2016-1548 Security Bypass Vulnerability | June 6, 2017 | SUNWntp4u | 143725-09 | 143725-09 and above |
| 63474 | CVE-2016-4957 | NTP CVE-2016-4957 Incomplete Fix Denial of Service Vulnerability | June 6, 2017 | SUNWntp4u | 143725-09 | 143725-09 and above |
| 63526 | CVE-2016-3115 | OpenSSH CVE-2016-3115 Remote Command Injection Vulnerability | June 6, 2017 | SUNWesu | 148104-23 | 148104-23 and above |

| VTM ID | CVE ID | CVE description | Due Date | Package information | Patch Number | Superseding Patch Information |
|--------|--------|----------------|----------|---------------------|--------------|------------------------------|
| 63896 | CVE-2015-8781/ CVE-2015-8782/ CVE-2015-8783 | LibTIFF Multiple Out of Bounds Memory Corruption Vulnerabilities | June 6, 2017 | SUNWPython | 119900-18 | 119900-18 and above |
| 63900 | CVE-2015-1547 | LibTIFF 'libtiff/tif_next.c' Memory Corruption Vulnerability | June 6, 2017 | SUNWPython | 119900-18 | 119900-18 and above |
| 65301 | CVE-2016-6491 | ImageMagick CVE-2016-6491 Remote Buffer Overflow Vulnerability | June 6, 2017 | SUNWimagickS | 136882-04 | 136882-04 and above |
| 65303 | CVE-2016-5841 CVE-2016-5842 | ImageMagick Integer Overflow and Information Disclosure Vulnerabilities | June 6, 2017 | SUNWimagickS | 136882-04 | 136882-04 and above |
| 65305 | CVE-2016-4971 | GNU Wget CVE-2016-4971 Arbitrary File Overwrite Vulnerability | June 6, 2017 | SUNWsfman SUNWwgetu | 125215-07 | 125215-07 and above |
| 65307 | CVE-2016-2177 | OpenSSL CVE-2016-2177 Integer Overflow Vulnerability | June 6, 2017 | SUNWwbsup | 150383-16 | 150383-16 and above |
| 65315 | CVE-2016-0718 | Expat CVE-2016-0718 Buffer Overflow Vulnerability | June 6, 2017 | SUNWlexpt | 137147-08 | 137147-08 and above |
| 59674 | CVE-2015-7575 | Mozilla Network Security Services CVE-2015-7575 Security Bypass Vulnerability | June 6, 2017 | SUNWj6dmo | 152076-31 | 152076-31 and above /152077-31 and above |
| | | | | SUNWj6dmx | 152077-31 | |

| VTM ID | CVE ID | CVE description | Due Date | Package information | Patch Number | Superseding Patch Information |
|---|---|---|---|---|---|---|
| 62092 | CVE-2016-3427 | Oracle Java SE and JRockit CVE-2016-3427 Remote Security Vulnerability | March 22, 2017 | SUNWj6dmo | 152076-31 | 152076-31 and above /152077-31 and above |
| | | | | SUNWj6dmx | 152077-31 | |
| 62109 | CVE-2016-0687 | Oracle Java SE CVE-2016-0687 Remote Security Vulnerability | March 22, 2017 | SUNWj6dmo | 152076-31 | 152076-31 and above /152077-31 and above |
| | | | | SUNWj6dmx | 152077-31 | |
| 62132 | CVE-2016-0686 | Oracle Java SE CVE-2016-0686 Remote Security Vulnerability | March 22, 2017 | SUNWj6dmo | 152076-31 | 152076-31 and above /152077-31 and above |
| | | | | SUNWj6dmx | 152077-31 | |
| 62144 | CVE-2016-3443 | Oracle Java SE CVE-2016-3443 Information Disclosure Vulnerability | March 22, 2017 | SUNWj6dmo | 152076-31 | 152076-31 and above /152077-31 and above |
| | | | | SUNWj6dmx | 152077-31 | |
| 62197 | CVE-2016-3449 | Oracle Java SE CVE-2016-3449 Remote Security Vulnerability | June 6, 2017 | SUNWj6dmo | 152076-31 | 152076-31 and above /152077-31 and above |
| | | | | SUNWj6dmx | 152077-31 | |
| 62213 | CVE-2016-3425 | Oracle Java SE and JRockit CVE-2016-3425 Remote Security Vulnerability | June 6, 2017 | SUNWj6dmo | 152076-31 | 152076-31 and above /152077-31 and above |
| | | | | SUNWj6dmx | 152077-31 | |
| 62225 | CVE-2016-3422 | Oracle Java SE CVE-2016-3422 Remote Security Vulnerability | June 6, 2017 | SUNWj6dmo | 152076-31 | 152076-31 and above /152077-31 and above |
| | | | | SUNWj6dmx | 152077-31 | |
| 64551 | CVE-2016-3503 | Oracle Java SE CVE-2016-3503 Local Security Vulnerability | June 6, 2017 | SUNWj6dmo | 152076-31 | 152076-31 and above /152077-31 and above |
| | | | | SUNWj6dmx | 152077-31 | |

| VTM ID | CVE ID | CVE description | Due Date | Package information | Patch Number | Superseding Patch Information |
|---|---|---|---|---|---|---|
| 64583 | CVE-2016-3508 | Oracle Java SE and JRockit CVE-2016-3508 Remote Security Vulnerability | June 6, 2017 | SUNWj6dmo | 152076-31 / | 152076-31 and above /152077-31 and above |
| | | | | SUNWj6dmx | 152077-31 | |
| 64595 | CVE-2016-3500 | Oracle Java SE and JRockit CVE-2016-3500 Remote Security Vulnerability | June 6, 2017 | SUNWj6dmo | 152076-31 | 152076-31 and above /152077-31 and above |
| | | | | SUNWj6dmx | 152077-31 | |
| 66703 | CVE-2016-5556 | Oracle Java SE CVE-2016-5556 Remote Security Vulnerability | January 17, 2017 | SUNWj6dmo | 152076-31 | 152076-31 and above /152077-31 and above |
| | | | | SUNWj6dmx | 152077-31 | |
| 66717 | CVE-2016-5568 | Oracle Java SE CVE-2016-5568 Remote Security Vulnerability | January 17, 2017 | SUNWj6dmo | 152076-31 | 152076-31 and above /152077-31 and above |
| | | | | SUNWj6dmx | 152077-31 | |
| 66731 | CVE-2016-5582 | Oracle Java SE CVE-2016-5582 Remote Security Vulnerability | January 17, 2017 | SUNWj6dmo | 152076-31 | 152076-31 and above /152077-31 and above |
| | | | | SUNWj6dmx | 152077-31 | |
| 66745 | CVE-2016-5573 | Oracle Java SE CVE-2016-5573 Remote Security Vulnerability | January 17, 2017 | SUNWj6dmo | 152076-31 | 152076-31 and above /152077-31 and above |
| | | | | SUNWj6dmx | 152077-31 | |
| 66828 | CVE-2016-5597 | Oracle Java SE CVE-2016-5597 Remote Security Vulnerability | May 5, 2017 | SUNWj6dmo | 152076-31 | 152076-31 and above /152077-31 and above |
| | | | | SUNWj6dmx | 152077-31 | |