

Oracle Solaris 11.3.36.24.0 Limited Support Update (Oracle Solaris 11.3 LSU 36.24.0) (Doc ID 2743496.1)

In this Document

[Main Content](#)

[Contents](#)

[Why Apply Oracle Solaris 11.3.36.24.0](#)

[Before Installing Oracle Solaris 11.3.36.24.0](#)

[Bugs Fixed](#)

[Packages Updated](#)

[Superseded IDRs](#)

[About Oracle Solaris 11 Limited Support Updates](#)

[Determining the Oracle Solaris Version Installed on Your System](#)

[Managing the Repository](#)

[How to Update Your Local Repository](#)

[Oracle Solaris Repository Reorganization](#)

[Further Assistance](#)

APPLIES TO:

Solaris x64/x86 Operating System - Version 11.3 to 11.3 [Release 11.0]

Solaris Operating System - Version 11.3 to 11.3 [Release 11.0]

Oracle Solaris on SPARC (64-bit)

Oracle Solaris on x86-64 (64-bit)

MAIN CONTENT

This README describes why you need to apply this LSU, caveats, and other important information that you might need to consider before applying or installing Oracle Solaris 11.3.36.24.0. It also contains general information about Oracle Solaris 11 Limited Support Update (LSU) and instructions about how to manage your local repository.

Contents

- [Why Apply Oracle Solaris 11.3.36.24.0](#)
 - [Before Installing Oracle Solaris 11.3.36.24.0](#)
 - [Bugs Fixed](#)
 - [Packages Updated](#)
 - [Superseded IDRs](#)
 - [About Oracle Solaris 11 Limited Support Updates](#)
 - [Determining the Oracle Solaris Version Installed on Your System](#)
 - [Managing the Repository](#)
 - [How to Update Your Local Repository](#)
 - [Oracle Solaris Repository Reorganization](#)
 - [Further Assistance](#)
-

Why Apply Oracle Solaris 11.3.36.24.0

Oracle Solaris 11.3.36.24.0 provides improvements and bug fixes that are applicable for all the Oracle Solaris 11 systems. Where possible we recommend that you update to Oracle Solaris 11.4. For those that need to stay on Oracle Solaris 11.3, the recommendation is to update to Oracle Solaris 11.3.35 first before installing the LSU. Some of the noteworthy improvements in this LSU include:

- FreeType has been updated to 2.10.4, and addresses a security issue (Bugs 32047869, 32047894)
- OpenSSL has been updated to 1.0.2x, and addresses security issues (Bugs 32247243, 31899422, 32247269)

For a complete list of bugs fixed in this LSU, see [Bugs Fixed](#).

For the list of Service Alerts affecting each Oracle Solaris 11.3 LSU, see [Important Oracle Solaris 11.3 SRU Issues \(Doc ID 2076753.1\)](#).

Note: Updated Java 7/8 packages are available but not included in the LSU repository zip image. See [Note 1](#) for the location and details on how to update Java. For more information and bugs fixed, see [Java 8 Update 281 Release Notes](#) and [Java 7 Update 291 Release Notes](#). For further details regarding Java and Oracle Solaris, see [Java Patches for Solaris Packages Contents](#).

Before Installing Oracle Solaris 11.3.36.24.0

This section provides some information about special installation and runtime instructions that you need to consider before installing or running Oracle Solaris 11.3.36.24.0.

Note 1: Installing updated Java versions

The latest Java packages are available in the support repository at <https://pkg.oracle.com/solaris/support>. They are also available as a separate download at [Java Patches for Solaris Packages \(Doc ID 1397756.1\)](#). If newer versions are listed in this document, proceed with performing the following steps to update to the latest versions of Java.

To update Java 8 packages:

```
# pkg change-facet version-lock.consolidation/java-8/java-8-incorporation=false
# pkg update jre-8
```

To update Java 7 packages:

```
# pkg change-facet version-lock.consolidation/java-7/java-7-incorporation=false
# pkg update jre-7
```

The release of Oracle Solaris 11.3 has obsoleted the use of Java 6 packages such that they are removed upon installation. By default, Java 8 will be the active version of Java on the system. It is strongly advised that systems do not run Java 6 but move to using a newer release of Java which helps in utilizing many modern features and increasing performance. However, if there is still a need to use Java 6, the following steps can be performed to install it:

Unlock the package:

```
# pkg change-facet version-lock.consolidation/ub_javavm-6/ub_javavm-6-incorporation=false
```

Update the incorporation package to the older version:

```
# pkg update consolidation/ub_javavm-6/ub_javavm-6-incorporation@1.6.0.115
```

Note: The version of the package at the end of the FMRI may change when new versions of Java 6 becomes available.

Freeze the incorporation package to prevent it from being removed on subsequent updates:

```
# pkg freeze ub_javavm-6-incorporation@1.6.0.115
```

Install the Java 6 runtime package:

```
# pkg install runtime/java/jre-6
```

If required, set the default version of Java to be Java 6:

```
# pkg set-mediator -V 1.6 java
```

These steps will let you use Java 6 as the default version of Java. However, it is highly recommended to install and use the later versions of Java.

Note 2: Support for NVIDIA Legacy Drivers in Oracle Solaris

The NVIDIA graphics driver is updated to version 346.35, which supports the recent family of NVIDIA GPUs. The NVIDIA legacy drivers are available in the repository as `driver/graphics/nvidiaR340` and `driver/graphics/nvidiaR304`

packages. For information about the support for legacy GPUs, see http://www.nvidia.com/object/IO_32667.html.

For GPUs that need the R340 legacy driver, you can install R340 by using the following command:

```
# pkg install --reject driver/graphics/nvidia driver/graphics/nvidiaR340
```

For GPUs that need the R304 legacy driver, you can install R304 by using the following command:

```
# pkg install --reject driver/graphics/nvidia driver/graphics/nvidiaR304
```

For more information, see the `/usr/share/doc/NVIDIA/README.txt` file.

Note 3: Updating to OpenSSH 7.1p1 (Oracle Solaris 11.3.5) or OpenSSH 7.2p2 (Oracle Solaris 11.3.9)

The update to Oracle Solaris 11.3.5 makes important changes to the default list of allowed cryptographic mechanisms for OpenSSH. Since the default implementation of Secure Shell in Oracle Solaris 11.3 is `sunssh`, most systems will not be affected by this change.

However, if `pkg mediator ssh` shows `openssh` in use, then security changes to the default allowed behavior could prevent `ssh` in and/or out of the machine from older operating environments until either remote or local changes are made. These remote or local changes need to be made to keys, and/or configuration files.

If `pkg mediator ssh` shows `sunssh` as the implementation, or shows `No matching mediators found`, then these OpenSSH changes will not impact the system. OpenSSH and the `ssh` mediator were introduced in Oracle Solaris 11.3.

OpenSSH provides some ciphers that SunSSH does not provide. These ciphers are less common. If you are using any of these ciphers from OpenSSH, then temporarily switch to SunSSH using the mediator mechanism. You can then adjust the legacy systems. For more information and a list of OpenSSH-only ciphers, see 'Unsafe Algorithms Removed' below.

To switch to `sunssh`, use the following command:

```
# pkg set-mediator -I sunssh ssh
```

Please make sure that you investigate, test, and make the necessary changes before moving back to OpenSSH.

If you are using OpenSSH and are installing this SRU, please check for the following security considerations:

- **ssh-dss Keys Disabled by Default**

The `ssh-dss` and `ssh-dss-cert-*` host and user key types are inherently weak and are disabled by default at run time.

If the `ssh-rsa` and `ssh-dss` host keys are not already present, use the `svc:/network/ssh:default` to create both the keys. It is unusual for Oracle Solaris servers to have the `ssh-dss` host keys but not the `ssh-rsa` keys.

If you have been using `ssh-dss` keys for public key authentication, you should create new `ssh-rsa` keys and remove the existing `ssh-dss` keys from all `authorized_keys` files. For information about creating new keys, see the `ssh-keygen(1)` man page.

- **diffie-hellman-group1-sha1 Key Exchange Disabled by Default**

The `diffie-hellman-group1-sha1` key exchange is no longer considered secure, and is disabled on both the client and the server.

If systems do not have a matching `kex` algorithm between the server and the client, you will receive the `no kex alg error`.

If your servers support only the `diffie-hellman-group1-sha1` key exchange, you should upgrade them to support `diffie-hellman-group-exchange-sha256`. You can also upgrade Oracle Solaris to a version which supports the `diffie-hellman-group14-sha1` key exchange.

If upgrading the peer is not an option, users connecting to systems that do not support the `diffie-hellman-group-exchange-sha256`, the `diffie-hellman-group14-sha1`, or the `diffie-hellman-group-exchange-sha1` key exchanges can explicitly enable the `diffie-hellman-group1-sha1` as follows:

```
root@source# ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 user@somehost
```

The server administrator can allow logins from systems that do not support secure key exchange methods by explicitly enabling insecure key exchange methods. Add the following lines to the `/etc/ssh/ssh_config` file (or a user's `.ssh/ssh_config` file) and restart the SSH server:

```
# Keep this file compatible with both sunssh and Openssh
IgnoreUnknown IgnoreIfUnknown
IgnoreIfUnknown IgnoreUnknown, KexAlgorithms

# Enable legacy algorithms -- remove when no longer needed.
KexAlgorithms
diffie-hellman-group1-sha1,diffie-hellman-group14-sha1,diffie-hellman-group-exchange-sha1,diffie-
hellman-group-exchange-sha256
```

- SSH Protocol 1 Support Removed

In Oracle Solaris 11.3.5, SSH-1 support has been removed on both the server side and the client side. Network entities that support only SSH-1 are mostly old network routers. You can no longer connect to such devices by using OpenSSH. However, you can still use SunSSH to access systems that use SSH-1.

- Unsafe Algorithms Removed

The default list of enabled ciphers and MACs is reduced for `sshd` in OpenSSH 7.1p1 to remove unsafe algorithms, and further reduced for clients in OpenSSH 7.2p2, but the total list remains the same. Any ciphers or MACs needed can be re-enabled using the `ciphers` and `MACs` options to configure the files. For more information, see the `man ssh_config(4)` and `man sshd_config(4)` man pages.

If the ciphers needed at the site are also available in `sunssh`, then reverting to `sunssh` is another workaround that can be used until peer systems can be upgraded to use stronger algorithms.

The following OpenSSH ciphers are not available in `sunssh`:

```
aes128-gcm@openssh.com
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com
rijndael-cbc@lysator.liu.se (not used in OpenSSH 7.1p1 by default)
```

Ciphers available in OpenSSH 7.1p1 by default. The recommended ciphers to be used are:

The default Ciphers list for `sshd`:

```
chacha20-poly1305@openssh.com
aes128-ctr
aes192-ctr
aes256-ctr
aes128-gcm@openssh.com
aes256-gcm@openssh.com
```

The default Ciphers list for `ssh` is the same as `sshd` plus:

```
aes128-cbc
3des-cbc
aes192-cbc
aes256-cbc
```

MACs:

MACs available in OpenSSH 7.1p1 `sshd` (server) by default. The recommended MACs to be used are:

The default MACs list for `sshd`:

```
umac-64-etm@openssh.com
umac-128-etm@openssh.com
hmac-sha2-256-etm@openssh.com
hmac-sha2-512-etm@openssh.com
hmac-sha1-etm@openssh.com
umac-64@openssh.com
umac-128@openssh.com
```

```

hmac-sha2-256
hmac-sha2-512
hmac-sha1

```

Formerly allowed `ssh` client additions to the above list are disabled by default in OpenSSH 7.2p2.

The impact on interoperability is minimal due to the use of other popular algorithms that remain enabled by default.

In particular, this change does not affect interoperability with older Oracle Solaris releases. Even SunSSH on Solaris 9 has a choice of common ciphers (`aes128-cbc`, `3des-cbc`) and a common MAC (`hmac-sha1`) with the OpenSSH 7.2p2 client in default configuration.

OpenSSH 7.2p2 also re-enables Ed25519 based cryptography in OpenSSH. The `curve25519-sha256@libssh.org` key exchange method and `ssh-ed25519` key type are also newly available for use after upgrading to this SRU.

You can use the following commands with OpenSSH to list all supported ciphers and MACs:

```
root@source# ssh -Q cipher
```

```
root@source# ssh -Q mac
```

- Default Value of `UseDNS` is No.

If no `UseDNS` value is specified in the `sshd_config` file, the default value of `UseDNS` is No. The former default value used to provide no security benefit.

A `UseDNS` value of No means that you cannot use host names when configuring an `ssh` service.

You have two options:

- You can explicitly specify `UseDNS yes` in the `sshd_config` file.
- You can use IP addresses instead of host names in the `sshd_config` file as shown in the following examples.

In the Match block section of the `sshd_config` file, use an Address criterion instead of a Host criterion. For example, you can replace `Match Host somehost.domain` with `Match Address 192.168.0.10`.

In the `sshd_config` entries for `AllowUsers`, `AllowGroups`, `DenyUsers`, and `DenyGroups`, use an IP address instead of the host name. For example, you can replace `AllowUsers jsmith@somehost.domain` with `AllowUsers jsmith@192.168.0.10`.

In `/etc/ssh/shosts.equiv` or `~/.shosts` entries, use an IP address instead of a host name. For example, you can replace `somehost.domain` with `192.168.0.10`.

In the `~/.ssh/authorized_keys` entry, use an IP address instead of a host name if specifying the `from` option. For more information, see the `man sshd(1M)` man page. For example, you can replace `from="somehost.domain" ssh-rsa AAAAB3...Q== jsmith@work` with `from="192.168.0.10" ssh-rsa AAAAB3...Q== jsmith@work`

- TCP Wrappers such as `hosts.deny` and `hosts.allow` are not supported for OpenSSH

The `openssh` implementation of Secure Shell no longer supports TCP wrappers. You will need to modify the `sshd_config` file or use a firewall to preserve a configuration that was previously enforced by TCP wrappers.

(Note: The `openssh` implementation of Secure Shell continues to use TCP connections. However, the TCP wrapper function, `libwrap`, is no longer supported.)

If you use TCP wrappers, you are using `/etc/hosts.allow` or `/etc/hosts.deny` to allow or deny logins. Instead, you can use the Match block in the `sshd_config` file to set up an equivalent configuration.

For example, to allow logins only from the `10.163.0.0/16` subnet, you might have set up TCP wrappers as follows:

```

root@jsmith-cz:~# cat /etc/hosts.allow
sshd : 10.163.
root@jsmith-cz:~# cat /etc/hosts.deny
ALL : ALL

```

In a Match block in the `sshd_config` file, the following entry sets an equivalent restriction:

```
Match Address *,!10.163.0.0/16
MaxAuthTries 0
```

Another option is to use a firewall for access control. Settings similar to these examples can be applied on a firewall. Access control in the firewall occurs earlier, before the network connection is established in the kernel.

Note 4: Oracle Solaris 11.3.5 and OpenSSL 1.0.1r upgrade

In OpenSSL 1.0.1r, OpenSSL disallows the use of DH key smaller than 1024-bit. If the server is set up to use a DH key smaller than 1024-bit key, the SSL/TLS connection will fail with error messages similar to:

```
| Thu Feb 11 09:32:14.2501      Starting ldap_cachemgr, logfile
| /var/ldap/cachemgr.log
| Thu Feb 11 09:32:14.6968      sig_ok_to_exit(): parent exiting...
| Thu Feb 11 09:32:14.8270      Error: Unable to refresh
| profile:XXX-tls:Session error no available conn.
```

You may also see an error message like:

```
| error:14082174:SSL routines:ssl3_check_cert_and_algorithm:dh key too small
```

To resolve the issue, the server must be configured to use a stronger DH parameter where 2048-bit is the recommendation. Follow these steps for configuring the server:

Generate a 2048-bit DH parameter:

```
% openssl dhparam -out dhparams.pem 2048
```

Configure the server to use the new DH parameter, `dhparams.pem`. Configuring the DH parameter differs depending on the server.

For more information, see <https://weakdh.org/sysadmin.html>.

Note 5: Need a switch to turn off Exafusion/verb in Oracle Solaris (Bug 22027298)

The changes introduced in Bug 22027298 disables the use of userland RDMA through the InfiniBand stack using the OpenFabrics User Verbs APIs by default. This is necessary in order to prevent the Oracle Real Application Cluster (RAC) environment from using these interfaces which are pending certain new functionality.

If you have existing applications using OpenFabrics User Verbs APIs and are not running these applications on a node in an Oracle RAC, it is possible and necessary to re-enable the OpenFabrics User Verbs APIs by adding the following line to the `/etc/system` file and rebooting Oracle Solaris.

```
set sol_uverbs:__user_verbs_rdmacm_disabled=0x0
```

Note 6: sendfile not returning EOPNOTSUPP error for unsupported socket types (Bug 22609739)

In previous releases, `sendfile` would return an `EOPNOTSUPP` error on a UDP socket. Due to this bug, customers will no longer get this error. However, the behavior for TCP socket remains unchanged.

Note 7: Updating to the latest timezone package

The latest timezone package is available in the support repository at <https://pkg.oracle.com/solaris/support>. It is also available as a separate download at [Timezone Data File Package for Oracle Solaris 11 \(Doc ID 2135137.1\)](#). If a newer version is listed in this document, proceed with performing the following steps to update to the latest timezone package.

Unlock the timezone package from the constraints on the system:

```
# pkg change-facet version-lock.system/data/timezone=false
# pkg update timezone
```

Note: When a package is unlocked, it may no longer be updated when the system is updated depending upon how the update is performed. If the update is performed using the `pkg update entire@<sru number>` command, then the timezone package will not be updated. If the update is performed using the `pkg update` command, then the timezone package will be updated.

Once the SRU that contains the package is released, you can optionally rellock the package:

```
# pkg change-facet version-lock.system/data/timezone=none
```

Note 8: rfs4_lo_state_destroy needs Sun Cluster hook for lock removal (Bug 18431888)

Network Lock Manager is a service that provides file and record locking in an NFS environment. To support this functionality within the Clustered File System (PXFS), please install Oracle Solaris 11.3.8.

Note 9: Default umask setting for Apache Tomcat 8 (Bug 24347227)

Apache Tomcat 8 is now started by default with a more strict umask value of 0027. If this value is inconvenient, a different umask value can be set by the `UMASK` variable in `setenv.sh`. For more information, see the `tomcat8(1M)` man page.

Note 10: Moving from non-encrypted swap to encrypted swap

If there is already an unencrypted swap device configured using the `swap -l` command, but you plan to use encryption, then follow these steps for moving to the encrypted swap:

- Delete the swap device
- Edit `/etc/vfstab` to add the "encrypted" option
- Reboot the system

Note 11: Updating to Samba 4.4.x

Samba has updated from 3.6.x release to 4.4.x release. Backup your data before the Samba update in "ASCII mode" using the `-c` option in `cpio`, as the ID mapping of the Active Directory (AD) domain users can change.

Note 12: New Solaris 11.3 constraint package

A new convenience package has been released in Oracle Solaris 11.3.14. It can be installed using the following command:

```
# pkg install solaris-11.3
```

The purpose of this package is to prevent the update of the system to a later major version of Oracle Solaris, but to allow the system to continue to be updated on the Oracle Solaris 11.3 SRU stream of changes.

Note 13: Updated /etc/ssh/moduli in Oracle Solaris 11.3.15

This update replaces `/etc/ssh/moduli` if it has not been modified. The new `moduli` file has the advantage of being unique to this release of Oracle Solaris, and has longer keys than the older version.

Shorter keys are provided for backward compatibility, but the two shortest key sizes are commented-out.

It is recommended that the keys be tested before putting it into production, in case the production environment needs to communicate with very old machines that might need to be updated to accommodate longer keys. This issue was not seen in testing with the still-supported Oracle Solaris versions, but that cannot replicate all possible customer environments.

Size 1023 entries are commented-out and should not be used, but are provided in case of urgent and temporary legacy needs.

Size 1535 entries are commented-out as they will likely become obsolete soon, but are provided for legacy needs.

Note 14: CGI functionality with Perl 5.22

Install the `library/perl-5/CGI` package to get full CGI functionality with Perl 5.22:

```
# pkg install library/perl-5/CGI
```

Note 15: pflog - a log daemon for the Packet Filter (PF)

The network/firewall/firewall-pflog package delivers the pflogd daemon, which allows Packet Filter (PF) to log packets to the regular file /var/log/firewall/pflog/pflog0.pkt by default. The file can be processed by tshark/wireshark only. The PF logs packet, which matches a rule with the 'log' action. The pflogd process is managed by the svc:/network/firewall/pflog:default SMF service instance, which creates the temporal capture link at start up. The capture link transmits logged packets from the kernel to the pflogd process running in user space. For more information, see the pf.conf(5) and dladm(1M) man pages.

Note 16: "getent ethers" output should follow the format described in ethers(4) (Bug 22514343)

Oracle Solaris 11.3.17 fixes a bug in getent where "getent ethers" did not follow the format defined in ethers(4), as it previously followed the output format of "official-host-name ethernet-address". It now follows the format in ethers(4) which is "ethernet-address official-host-name".

Note 17: hotplug poweroff sometimes hit "ERROR: devices or resources are busy." (Bug 25752894)

An attempt to offline a hotplug port with dependent devices that are currently in use by the system might fail with the following error message:

```
# hotplug poweroff /pci@13c/pci@1/SYS/RCSA/PCIE11
ERROR: devices or resources are busy.
```

You are advised to wait two minutes for the active holds to be released before retrying the hotplug offline command:

```
# hotplug offline
```

This process must be repeated until the hotplug offline command succeeds.

Note 18: Oracle Solaris 11.3.20 and glib 2.46.0

With the upgrade of glib to 2.46.0 in Oracle Solaris 11.3.20, G_CONST_RETURN is now deprecated and should not be used. For more information, see <https://developer.gnome.org/glib/stable/glib-Standard-Macros.html#G-CONST-RETURN:CAPS>.

Note 19: Perl 5.22 and Perl 5.12 in Oracle Solaris 11.3.21

Oracle Solaris 11.3.21 contains a security fix for Perl 5.22 and Perl 5.12 (CVE-2016-1238). This fix affects how Perl scripts behave when loading the modules through the 'use' or 'require' directive. Before this fix was introduced, Perl loaded the module from the current path if it was not found in one of the standard directories. The fix removes this feature. In other words, @INC previously contained '.' as the last item, and now it does not. Unfortunately, this feature has been hard-coded in Perl for a very long time. Hence, the chance of introducing a regression is high.

There are several possibilities on how to make the scripts work depending on the old behavior:

- Use "use lib '.';".

This directive prepends '.' to @INC;. This means that '.' will be searched as the **first** directory, as it was the last directory before the fix. For more information, see /usr/perl5/bin/perl5doc lib'.

- Use the "-I ." command line parameter.

This prepends the '.' to the start of @INC.

- Use "BEGIN { push @INC, '.' }".

This appends '.' more closely mimicking the previous behavior.

- Use "require './module';".

The 'require' directive specifies the path directly.

- Disable the fix by exporting the PERL_USE_UNSAFE_INC environment variable.

```
export PERL_USE_UNSAFE_INC=1
perl myscript.pl
```

- Disable the fix globally by editing /etc/perl/sitecustomize.pl and commenting out the line "pop @INC ...".

Some Perl scripts are known to require modification due to the new fix. These are testing and benchmark scripts, which are included in these affected packages that are not installed by default:

```
benchmark/filebench
database/mysql-51/tests
database/mysql-55/tests
database/mysql-56/tests
database/mysql-57/tests
```

The required modifications are:

1. `/usr/benchmarks/filebench/bin/filebench`

You can override functionality defined in the `/usr/benchmarks/filebench/config/...` directory by creating a file in the current directory. This will also require you to update line 1045 in `/usr/benchmarks/filebench/bin/filebench` from `require "$function.func";` to `require ".$function.func";`.

2. `/usr/mysql/5.[1567]/mysql-test/mysql-test-run.pl`

Add `"use lib '.';"` before `"use strict;"` in `mysql-test-run.pl`.

Note 20: Change in FIPS 140-2 Cryptographic Provider for Kerberos Changes Non-Compliant Application Behavior in Oracle Solaris 11.3.21

Applications that are running in FIPS 140-2 mode in a Kerberos environment may behave differently in this release as the cryptographic provider has changed.

In earlier Oracle Solaris 11.3 SRU releases, the Cryptographic Framework was the provider for Kerberos, and the administrator was instructed to configure Kerberos to use only `des3-cbc-sha1`. If a Kerberos application did not use this enctype, the Cryptographic Framework issued a warning but did not abort the application.

In Oracle Solaris 11.3.21, the Kerberos implementation is MIT Kerberos, which uses the OpenSSL crypto provider. OpenSSL applications that run in FIPS 140-2 mode end up failing, and are aborted when a non-validated enctype is called. The following message is displayed in case of failure:

```
aes_misc.c(83): OpenSSL internal error, assertion failed: Low level API call to cipher AES forbidden in FIP
```

For instructions about how to configure Kerberos to use FIPS 140-2 validated encatypes only, see [Managing Kerberos and Other Authentication Services in Oracle Solaris 11.3](#).

For information about the differences between the two FIPS 140-2 crypto providers, see [About OpenSSL in FIPS 140-2 Mode in Oracle Solaris](#) and [About the Cryptographic Framework in FIPS 140-2 Mode](#).

Note 21: rpool/VARSHARE/zones missing in Oracle Solaris 11.3.22

If `zonepath` is not specified when creating Oracle Solaris 11 zones, the `zoneadm install` command will fail. The workaround is to set the `canmount` option and mount `rpool/VARSHARE/zones`, which will mount `./system/zones`. Use the following commands:

```
# zfs set canmount=on rpool/VARSHARE/zones
# zfs mount rpool/VARSHARE/zones
```

You can now install Oracle Solaris 11 non-global zones that do not specify a `zonepath`.

This issue only affects systems that are freshly installed with Oracle Solaris 11.3.22 or higher. Systems that are updated from earlier Oracle Solaris 11 SRUs to Oracle Solaris 11.3.22 are unaffected.

Note 22: Openstack Horizon and Oracle Solaris 11.3.23

Openstack Horizon fails to launch in Oracle Solaris 11.3.23. The workaround is to replace `'sys.path.append("/usr/lib/horizon/")'` with `'sys.path.insert(0, "/usr/lib/horizon/")'` in `/usr/lib/python2.7/vendor-packages/openstack_dashboard/wsgi/django.wsgi`, and then restart apache using the following command:

```
# svcadm restart svc:/network/http:apache24
```

Note 23: Netifaces 2.7 Python module segfaults on calling gateways()

Netifaces 2.7 python module segfaults on Oracle Solaris 11.3.20 and above. Oracle Solaris 11.3.24 corrects this issue on x86 platforms, but it might still be seen on SPARC. IDR3329.2 has been created to address this issue for SPARC servers. Please see [Adding and Updating Software in Oracle Solaris 11.3](#) for complete information on adding IDRs to your system.

1. Become an administrator

For more information, see [How to Use Your Assigned Administrative Rights in Securing Users and Processes in Oracle Solaris 11.3](#).

2. Add the package archive as a publisher origin.

```
$ pkg set-publisher -g idr3329.2.p5p solaris
```

3. Install the IDR

```
$ pkg install --backup-be-name pre-idr3329 idr3329
```

Note 24: Updating to OpenSSH 7.4p1 or later

This release includes a change that may affect existing configurations:

ssh(1): Remove 3des-cbc from the client's default proposal. 64-bit block ciphers are not safe in 2016 and we don't want to wait until attacks like SWEET32 are extended to SSH. As 3des-cbc was the only mandatory cipher in the SSH RFCs, this may cause problems connecting to older devices using the default configuration, but it's highly likely that such devices already need explicit configuration for key exchange and hostkey algorithms already anyway.

Note 25: Kernel Zones may fail to boot when upgrading T7 machines to Oracle Solaris 11.3.23 or later if system firmware is not up to date (Bug 24297395)

If you are running Kernel Zones on T7 machines installed with Oracle Solaris 11.3.23 or later, make sure the underlying hosts' firmware is up to date. If this is not performed, the Kernel Zones will fail to boot with:

```
zone '<name of zone>': hypervisor needs updating for DAX support in this zone
```

Note 26: Installing Oracle Instant Client

Oracle Solaris 11.3.26 comes with an updated version of the Oracle Instant Client packages and some package name changes. The package name changes enable installation of multiple concurrent versions of the Oracle Instant Client, which matches functionality available if downloading the Oracle Instant Client from Oracle Technical Network.

The original package names:

```
database/oracle/instantclient
database/oracle/instantclient/jdbc-supplement
database/oracle/instantclient/odbc-supplement
developer/oracle/instantclient/sdk
```

have been renamed to include the "-121" suffix, which contain Oracle Instant Client v12.1:

```
database/oracle/instantclient-121
database/oracle/instantclient/jdbc-supplement-121
database/oracle/instantclient/odbc-supplement-121
developer/oracle/instantclient/sdk-121
```

The new version of the Oracle Instant Client, v12.2, is available with these packages:

```
database/oracle/instantclient-122
database/oracle/instantclient/jdbc-supplement-122
database/oracle/instantclient/odbc-supplement-122
developer/oracle/instantclient/sdk-122
```

The utilities `sqlplus`, `adrci`, `uidrvci`, and `wrc` are now delivered to `usr/bin` as mediated links to either the 12.1 or 12.2 versions. You can check which version is active by running the `pkg mediator` command:

```
# pkg mediator instantclient
MEDIATOR      VER. SRC. VERSION IMPL. SRC. IMPLEMENTATION
instantclient local      12.1    local      vendor
```

For example:

```
$ man sqlplus
```

will give you the correct man page based on the mediator setting.

Note 27: ICU 59.1 in Oracle Solaris 11.3.26

For the list of changes between ICU 56.1 and 59.1, see the [ICU web site](#). The library is now built with the GNU project C++ compiler so make sure `icu-config(1)` or `pkg-config(1)` is used to determine the correct build flags.

Note 28: Oracle Solaris OCM package is no longer updated

The Oracle Solaris OCM package is no longer updated in the Oracle Solaris image. If you want to use the latest version please download it from MOS. See [OCM Package for Oracle Solaris 11 and Oracle Solaris 10](#) for further instructions.

Note 29: New GNU binutils in Oracle Solaris 11.3.33 (Bug 27028053)

The new GNU binutils in Oracle Solaris 11.3 delivers new gas which expects 64-bit asm by default. It could cause problem with older gcc versions like the following:

```
Error: invalid instruction suffix for `push`
```

You have to explicitly specify `-m32` for compilation. However, the recommendation is to use `gcc5` for compilation to avoid this problem.

Note 30: Remote RAD and auto-generated SSL certificate in Oracle Solaris 11.3.34

If you are using remote RAD with auto-generated SSL certificate that was generated prior to Oracle Solaris 11.3.34, it is highly recommended that the certificate be regenerated with a stronger key. Perform the following steps for the regeneration:

```
# disable svc:/system/rad:remote
# rm /etc/rad/cert.pem
# rm /etc/rad/key.pem
# enable svc:/system/rad:remote
```

Use the following command for the verification:

```
# openssl x509 -in /etc/rad/cert.pem -text
```

Note 31: Several IPS packages in Oracle Solaris 11.3 are not incorporated by their respective incorporations

There are several IPS packages in Oracle Solaris 11.3 that aren't incorporated by their respective incorporations. See [Doc ID 2525825.1](#) for more information on this.

[Contents](#)

Bugs Fixed

Each LSU provides bug fixes and incremental changes that are relative to the preceding release, for example Oracle Solaris 11.3. The following additional bugs are fixed in this LSU:

Bug	Synopsis
-----	----------

31899422	Problem with library/openssl
32047869	update FreeType to 2.10.4
32047894	Problem with x11/font
32247243	Upgrade OpenSSL version to 1.0.2x
32247269	Problem with library/openssl
32354353	wanboot manifest update for OpenSSL 1.0.2x

For the complete Oracle Solaris 11.3 release history, see [Oracle Solaris 11.3 LSU Index](#).

- [Oracle Solaris 11.3.36.3.0 ReadMe \(Doc ID 2457998.1\)](#)
- [Oracle Solaris 11.3.36.7.0 ReadMe \(Doc ID 2492416.1\)](#)
- [Oracle Solaris 11.3.36.10.0 ReadMe \(Doc ID 2531260.1\)](#)
- [Oracle Solaris 11.3.36.13.0 ReadMe \(Doc ID 2565307.1\)](#)
- [Oracle Solaris 11.3.36.15.0 ReadMe \(Doc ID 2597494.1\)](#)
- [Oracle Solaris 11.3.36.18.0 ReadMe \(Doc ID 2628509.1\)](#)
- [Oracle Solaris 11.3.36.20.0 ReadMe \(Doc ID 2657274.1\)](#)
- [Oracle Solaris 11.3.36.21.0 ReadMe \(Doc ID 2686738.1\)](#)
- [Oracle Solaris 11.3.36.23.0 ReadMe \(Doc ID 2721603.1\)](#)

[Contents](#)

Packages Updated

The following packages are updated in this LSU:

Package	Summary
firmware/system/fallback-boot	Fallback Boot image
library/security/openssl	OpenSSL - a Toolkit for Secure Sockets Layer (SSL v2/v3) and Transport Layer (TLS v1) protocols and general purpose cryptographic library
library/security/openssl/openssl-fips-140	FIPS 140-2 Capable OpenSSL libraries
support/critical-patch-update/solaris-11.3-cpu	Oracle Solaris 11.3.36.24.0 Critical Patch Update 2021.1-1
system/boot/wanboot	WAN boot support
system/kernel/platform	Core Solaris Kernel Architecture
system/library/freetype-2	FreeType 2 font engine

[Contents](#)

Superseded IDRs

When a bug fix that is included in an Interim Diagnostic Relief (IDR) is addressed in a LSU, the IDR is superseded. Prior to updating this LSU, you do not necessarily need to remove the IDR that has been superseded. Running the pkg update command updates the system to the latest LSU and removes the relevant IDR from the system. However, the update fails if an IDR exists in the system and the IDR has not been superseded. There are no superseded IDRs for this LSU.

[Contents](#)

About Oracle Solaris 11 Limited Support Updates

Oracle Solaris 11 uses an Image Packaging System (IPS) repository to update all packages that are available in your system. Oracle Solaris 11.4 is the next installment in our ongoing support train for Oracle Solaris 11 and there will be no further Oracle Solaris 11.3 SRUs delivered to the support repository. However, for customers that are unable to update to Oracle Solaris 11.4 due to the EOL of features or hardware support in 11.4, limited support updates (LSUs) will be provided to deliver fixes required by Service Requests for these customers and also to deliver critical security fixes. LSU's will be available as a zip file download from My Oracle Support.

The update path for Oracle Solaris 11 users is to update to Oracle Solaris 11.3.35 and apply subsequent LSUs. For the complete list of Oracle Solaris 11.3 LSUs and downloads, see [Oracle Solaris 11.3 LSU Index](#).

Some important points to consider before applying or installing LSUs:

- LSUs can be installed on systems covered by an appropriate Oracle support contract.
- LSUs are updates to Oracle Solaris, but are not complete images. They provide bug fixes and incremental changes that are relative to the preceding release, for example Oracle Solaris 11.3.
- The LSU repository must include the base packages for the Oracle Solaris 11 Update that they apply to.
- If a subset of the LSUs are added to a repository, only those LSUs can be installed provided that the corresponding Oracle Solaris 11 Update base packages are included in the repository.
- If the base packages for the relevant Oracle Solaris 11 Update are not included in the repository containing the LSUs, failures will occur during various packaging operations.
- LSUs are released and available for download on a quarterly basis.
- The LSU release date coincides with Oracle's quarterly Critical Patch Update (CPU). The [CPU Documentation](#) references security vulnerabilities fixed in each LSU. This Critical Patch Update Advisory lists all relevant Oracle products.

To see the latest CPU, click the Critical Patch Update listed in the table. To see the security vulnerabilities that are fixed in recent Oracle Solaris LSUs, scroll down in the CPU document and click the "Oracle and Sun Systems Products Suite" link. This document also has a reference section to historical information for older Oracle Solaris SRUs and LSUs.

- LSUs must be applied during proactive maintenance to prevent issues, or when asked by Oracle Support for reactive break/fix maintenance situations. Customers should schedule such maintenance windows at least in line with the Oracle Critical Patch Update cycle, or more frequently as required by the industry and/or company compliance requirements. Note also that at times Oracle may release security vulnerability fixes outside of the normal Critical Patch Update cycle.
- If a system has an Interim Diagnostic Relief (IDR) installed, check if the issues addressed by the IDR are fixed in the LSU that you plan to install. If the issues are not fixed, you need to request a new IDR for that LSU several weeks in advance of the planned maintenance window.
- The LSU zip files on MOS provide an alternative download option to synchronize network based repository.

For latest support products news, and LSU availability email notifications, use the [My Oracle Support Hot Topics E-Mail](#) feature.

For a complete list of Oracle Solaris 11.3 LSUs and downloads, see [Oracle Solaris 11.3 LSU Index](#).

For instructions about applying LSUs to a system and managing a package repository, see [Managing The Repository. Contents](#)

Determining the Oracle Solaris Version Installed on Your System

To check the Oracle Solaris version installed on your system, use the pkg list entire command.

```
# pkg list entire
NAME (PUBLISHER)  VERSION
entire            0.5.11-0.175.3.36.0.3.0
```

Oracle Solaris LSU versions follow a naming convention similar to other Oracle applications such as MOS and BugDB. They follow the 5-digit Release.Update.SRU.Build.Respin format. In the example, 0.5.11-0.175.3.36.0.3.0 indicates Oracle Solaris 11.3, LSU version 36, build 3, and no respin.

For more information, see the [Oracle Solaris 11 package branch version scheme. Contents](#)

Managing the Repository

Some important points to consider before applying or installing the repository zip file:

- The minimum OS level required for the system to run this repository is Oracle Solaris 11.3.
- The repository is provided as zip files. They contain only the packages that have been updated in the LSU.
- This LSU is provided in two parts: Oracle Solaris IPS Repository Installation Guide and Oracle Solaris IPS Repository. The Oracle Solaris IPS Repository Installation Guide contains the install script and readme files. The Oracle Solaris IPS Repository contains the zip files of the repository. You must download both the parts from [MOS](#) to add the packages to an existing repository that contains Oracle Solaris 11.3.35.
- The zip file associated with this README must be used in conjunction with an existing local copy of the Oracle Solaris support repository that contains Oracle Solaris 11.3.35.
- It is necessary to have a valid `solaris` publisher set before performing an update. For instructions to create an Oracle Solaris 11.3 package repository, see [Copying and Creating Oracle Solaris 11.3 Package Repositories](#).

The example commands listed in this section should be executed with root privileges or by using `sudo(8)` or `pfexec(1)` commands.

How to Update Your Local Repository

Download the LSU's IPS Repository Installation Guide and IPS Repository patches from MOS.

Perform the following steps to update your local system with the contents of the LSU zip file:

1. Become an administrator.

For more information, see [How to Use Your Assigned Administrative Rights in Securing Users and Processes in Oracle Solaris 11.3](#).

2. Run the `install-repo.ksh` script that is included in the IPS Repository Installation Guide patch to update your existing repository.

```
$ install-repo.ksh [-c] [-v] -d full_path_to_existing_s11_3_repo
```

For example:

```
$ install-repo.ksh -c -v -d /export/support-repo
```

3. If the repository is managed by `pkgserve`, restart the appropriate service.

```
$ svcadm restart svc:/application/pkg/server:your_repo_instance
```

4. If an existing repository is not set, add the repository to the system.

```
$ pkg set-publisher -g file:///full_path_to_existing_s11_3_repo solaris
```

5. Update the packages.

```
$ pkg update
```

For more information about using the `install-repo.ksh` script, see the `README-zipped-repo.txt` file.

For more information about managing your repository, see the following resources:

- [Updating and Maintaining Oracle Solaris 11](#)
- [Oracle Solaris 11 Image Packaging System \(IPS\) Frequently Asked Questions \(FAQ\)](#)

Contents

Oracle Solaris Repository Reorganization

Over the past few years the release and particularly the support repositories for Oracle Solaris have grown considerably as new releases and SRUs have been added. Users who copy our entire repositories via `pkgrecv` may be downloading many packages that they will not need and this leads to increased download times. In the coming weeks we'll be pruning the Oracle Solaris 11.2 and older packages from the support and release repositories.

However, we realize that some folks might still need access to this (rather old) software and so that can be accessed via two new repositories:

```
http://pkg.oracle.com/solaris/legacy/release
https://pkg.oracle.com/solaris/legacy/support
```

Note: You can configure these repositories as before, just specifying the new URI/Origins. For the legacy/support repository, use your existing certificate/key pair.

[Contents](#)

Further Assistance

The documentation for Oracle Solaris 11.3 can be found at: [Oracle Solaris 11.3 Information Library](#).

If you have a support plan with Oracle, please contact your service representative for further assistance. Community discussion of this product can be found at:

[My Oracle Support Community - Oracle Solaris Installation, Booting, and Patching](#)

[Contents](#)

◀ ▶

Didn't find what you are looking for?