# Packages - Bug #3371

Bug # 3372 (fixed): [various]: error while loading shared libraries: libcrypto.so.1.1: cannot open shared object file: No such file or directory - may require chrooting

## cryptsetup/openssl update causing whirlpool-hashed LUKS boot failure

2022-11-09 09:30 AM - wael

| | | | |
|---|---|---|---|
| **Status:** | fixed | **% Done:** | 90% |
| **Priority:** | bug | | |
| **Assignee:** | bill-auger | | |
| **Category:** | | | |

**Description**

Forking off from issue #3368 as the scope is different (as bill-auger pointed out).
I've found that this is indeed caused by OpenSSL marking whirlpool as legacy and moving it to the legacy provider.
Yet the details aren't fully clear, according to cryptsetup documentation it relies on libgcrypt, which seems to be yet to deprecate whirlpool.
Anyone affected by the boot bug, please chime in with details of your setup so we might be able to unravel the root cause.

### History

**#1 - 2022-11-09 10:04 PM - bill-auger**

*- Parent task set to #3372*

*- Assignee set to bill-auger*

*- Status changed from unconfirmed to in progress*

**#2 - 2022-11-10 01:07 AM - bill-auger**

> Forking off from issue #3368 as the scope is different

unfortunately, the information needed to diagnosis and confirm the issue is conflated into the other ticket - TLDR: the solution is to install 'openssl-1.1'

symptoms apparent in log:

```
systemd-cryptsetup[170]: Requested LUKS hash whirlpool is not supported.
systemd-cryptsetup[170]: Failed to load LUKS superblock on device /dev/disk/by-uuid/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx: Invalid argument
```

whirlpool support in openssl can be checked with:

```
## openssl v1.1:
$ openssl     dgst -list | grep -o whirlpool
whirlpool

## openssl-1.1 v1.1:
$ openssl-1.1 dgst -list | grep -o whirlpool
whirlpool

## openssl v3:
$ openssl     dgst -list | grep -o whirlpool
```

The hash algorithm in use by LUKS can be checked with:

```
# cryptsetup luksDump /dev/sdAN | grep whirlpool
```

**#3 - 2022-11-10 08:52 AM - wael**

Long-term what is the solution though?
Re-encrypting the device and avoiding whirlpool or should Parabola move to using gnutls?
On the one-hand the first option will avoid the problem for sure, and the second solution is more overhead for the maintainers.
Yet, judging with the number of CVEs that keep popping up in OpenSSL, gnutls might be giving another advantage here.
Specifically since OpenSSL seems to be deprecating code solely because they don't want to deal with maintaining it - not because of some

cryptographic security reasoning.

**#4 - 2022-11-11 09:02 PM - wael**

I found the bug report from Arch:
https://bugs.archlinux.org/task/76440

**#5 - 2022-11-11 11:09 PM - wael**

I just attempted to change the hash from whirlpool to sha512, ended up with an unbootable system.
Long term, if OpenSSL will drop whirlpool this leaves only two options:
1) Wipe and install again, with a different hash algorithm (hopefully they don't deprecate sha512).
2) Maybe compile cryptsetup with gnutls instead of openssl?

**#6 - 2022-11-13 02:25 AM - bill-auger**

> Long term, if OpenSSL will drop whirlpool this leaves only two options:

its not dropped, but moved into a legacy.so library, which actually
suggests that it will be retained for the foreseeable future

the initial cryptsetup+openssl3 rebuild did not include the 'legacy' library,
and was broken the same way for many arch users - the latest one does;
so this may be solved already for the long-term

**#7 - 2022-11-14 03:23 AM - bill-auger**

*- Status changed from in progress to forwarded upstream*

**#8 - 2022-11-14 03:31 AM - bill-auger**

*- % Done changed from 0 to 90*

**#9 - 2022-12-15 05:59 PM - bill-auger**

*- Status changed from forwarded upstream to fixed*

cryptsetup 2.5.0-4 fixed this