Alpine Linux - Bug #7265

libGL error: MESA-LOADER: failed to retrieve device information

05/04/2017 04:52 PM - Ned Flanders

Status:	Closed	**Start date:**	05/04/2017
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	3.6.1		
Affected versions:		**Security IDs:**	

Description

I found a bug with Mesa.
It works fine as root but fails as normal user.
I have 2 reproduction cases.
You must have mesa-demos installed.

Case 1

glxinfo | head

```
name of display: :0
libGL error: MESA-LOADER: failed to retrieve device information
libGL error: Version 4 or later of flush extension not found
libGL error: failed to load driver: i915
libGL error: MESA-LOADER: failed to retrieve device information
display: :0  screen: 0
direct rendering: Yes
```

But **sudo glxinfo** works correctly without any errors.

Case 2

glxgears

It gives the same errors as above and the gears don't load.
After a while my desktop freezes.
OTOH **sudo glxgears** works.

History

#1 - 05/12/2017 06:41 PM - Shiz ...

Could you provide an strace to help us diagnose the issue? You can perform one like this:

```
apk add strace && strace glxinfo 2>&1 > strace.log
```

And then uploading strace.log here.

#2 - 05/12/2017 06:42 PM - Shiz ...

Sorry, that should be:

```
apk add strace && strace glxinfo >strace.log 2>&1
```

.

#3 - 05/12/2017 07:31 PM - Ned Flanders

- File strace.log added

Thank you for the instructions.
The result is attached.

#4 - 05/12/2017 08:40 PM - Ned Flanders

- File permissions-hardened.log added

- File permissions-vanilla.log added

I found one more important piece of information.
This bug only exists on alpine-hardened.
On alpine-vanilla it works fine.
I send attached a comparison of some directories permissions between hardened and vanilla that may be the reason for the differences.

Some grsec setting may be the source of this bug.

#5 - 05/12/2017 10:19 PM - Shiz ...

Yes, it seems subsystem detection in libdrm fails because of the failing readlink() call. I think this is caused by grsecurity's GRKERNSEC_SYSFS_RESTRICT, which restricts non-root access to big parts of /sys.

I'm not sure what the best approach to solve this is, as there is no runtime-settable

```
/proc/sys/kernel/grsecurity
```

entry for this...

#6 - 05/22/2017 09:39 AM - Natanael Copa

- Status changed from New to Resolved

looks like there is a boot option for it: grsec_sysfs_restrict=0

#7 - 05/23/2017 06:36 PM - Carlo Landmeter

- Target version changed from 3.6.0 to 3.6.1

#8 - 06/01/2017 07:20 PM - Natanael Copa

- Status changed from Resolved to Closed

#9 - 10/05/2017 09:16 PM - Carlo Landmeter

It looks like chromium is facing the same issues and is because of the limitations disabling webgl[1][2]

ncopa, would it be an option to add this kernel option by default? Is this such a security risk?

#10 - 10/06/2017 07:31 AM - Natanael Copa

The sysfs does leak information that may be useful for an attacker, which is why grsecurity chose to lock it down.

In general, I prefer that we have locked/hardened/secure defaults and let users open up things they need, rather than having things open by default and let users lock down/harden their config to becomes more secure if they can.

Files

strace.log	69.6 KB	05/12/2017	Ned Flanders
permissions-hardened.log	7.14 KB	05/12/2017	Ned Flanders
permissions-vanilla.log	7.2 KB	05/12/2017	Ned Flanders