

Fuzzing OpenGL Shaders Can Lead To Some Wild Results

Written by [Michael Larabel](#) in [Standards](#) on 11 December 2016 at 07:28 AM EST. [29 Comments](#)

```
#version 400
layout(triangles, equal_spacing)
void main(void) {
    vec4 p0 = gl_in[0];
    vec4 p1 = gl_in[1];
    vec4 p2 = gl_in[2];

    vec3 p = gl_TessCoC;
    gl_Position = p0*p.
```

Alastair Donaldson at the Imperial College London has been working on testing OpenGL shader compilers across vendors and operating systems with OpenGL shader fuzzing and has been finding some surprising -- and sometimes comical -- results. The results so far are interesting and show how some small code changes can cause big problems for some OpenGL shader compilers.

The researcher began his series with [this Medium post](#) outlining their work at the UK university for working to provide automatic testing of OpenGL shader compilers via GLfuzz to spot problems with the driver stacks.

Going in alphabetical order, he [started with AMD](#). With AMD's Windows drivers he was able to cause a "Bluescreen of Death" via WebGL on a web-page within Chrome, bad image rendering in desktop OpenGL as well as WebGL in Chrome, and more details. There's also an oddity whereby writing code past a break statement can cause an image not to render.

When [testing Apple](#) his team was able to spot PowerVR driver issues to cause garbage rendering as well as making a slug to disappear.

That's as far as their publishing has gone so far but more driver vendors are coming up. It's already been a lot of interesting reading, so if you have time this weekend, check out Alastair Donaldson's [Medium page](#).

[29 Comments](#)



 Tweet

 Like 7

 Share

Related News

[Monado 21.0 Released As An Officially Conformant OpenXR Implementation](#)

[Khronos Releases SYCL 2020 For C++ Heterogeneous Parallel Programming](#)

[HDMI Forum Closing Public Specification Access Is Hurting Open-Source GPU Drivers](#)

[MIPI I3C Host Controller Interface Driver Comes To Linux 5.11](#)

[POCL 1.6 Released For Portable OpenCL Atop CPUs, Other Accelerators](#)

[Khronos Brings New Physically Based Rendering Materials Support To glTF](#)

About The Author



Michael Larabel is the principal author of Phoronix.com and founded the site in 2004 with a focus on enriching the Linux hardware experience. Michael has written more than 20,000 articles covering the state of Linux hardware support, Linux performance, graphics drivers, and other topics. Michael is also the lead developer of the Phoronix Test Suite, Phoromatic, and OpenBenchmarking.org automated benchmarking software. He can be followed via [Twitter](#) or contacted via [MichaelLarabel.com](#).

Popular News This Week

[Nintendo 64 Support Mailed In For The Linux 5.12 Kernel](#)

[Linux Mint Finds Many Of Its Users Are Running Behind On Security Updates](#)

[0 A.D. Real -Time Strategy Game Sees First Release In Nearly Three Years](#)

[KDE Plasma 5.21 Released With Better Wayland Support, Desktop Improvements](#)

[PipeWire 0.3.22 Released With Many Improvements](#)

[NVIDIA Launching "CMP" Cards For Professional Mining, Limits RTX 3060 Mining Potential](#)
[GTK 4.2 Releasing Next Month With Likely Introducing A New OpenGL Renderer](#)
[Experimental Wayland Support For Wine Now Sees More Functionality Working](#)

Latest Linux News

[Google Provides Funding For Linux Kernel Developers To Focus On Security](#)
[Compute Express Link 2.0 Support Sent In For Linux 5.12, Enabling CXL 2.0 Memory Devices](#)
[Ampere Making Progress On Open-Source Firmware For Their CPUs/Platform](#)
[Linux 5.13 Should See HP Platform Profile Support](#)
[Debian Launches A Debuginfod Server For Smoother Debugging Experience](#)
[Proposed GCC 12 Security Option Would Auto Initialize Automatic Variables](#)
[Clang LTO Support Merged For Linux 5.12 Including ARM64 + x86_64](#)
[Early Ubuntu 21.04 Benchmarks Point To Some Slides In Performances But Overall Flat](#)
[Firefox 86.0 Released With Total Cookie Protection, Stack Clash Protection](#)
[Radeon RADV Driver Enables Displayable DCC For Some Performance Benefit](#)
[GNOME Shell + Mutter 40 Beta Released With Wayland Improvements, Overview Redesign](#)

Show Your Support, Go Premium

Phoronix Premium allows ad-free access to the site, multi-page articles on a single page, and other features while supporting this site's continued operations.

Latest Featured Articles

[GCC 10 vs. GCC 11 Compiler Performance On AMD Zen 3](#)
[Arch-Based SalientOS + EndeavourOS Take On Clear/Fedora/Ubuntu With The Ryzen 9 5900X](#)
[OpenGL vs. Vulkan Performance For Portal 2 With Radeon Linux Graphics](#)

[LLVM Clang 12 Performance Benchmarks On AMD Ryzen 9 5950X](#)
[HP ZBook Studio G7 Aims To Attract Linux Developers, Data Scientists](#)

Support Phoronix

The mission at Phoronix since 2004 has centered around enriching the Linux hardware experience. In addition to supporting our site through advertisements, you can help by [subscribing to Phoronix Premium](#). You can also contribute to Phoronix through a [PayPal tip](#).

Phoronix Media

[Phoronix Test Suite](#)

[OpenBenchmarking.org](#)

[Phoromatic](#)

[LinuxBenchmarking.com](#)

Phoronix Premium

[Support Phoronix](#)

[While Having Ad-Free Browsing,](#)

[Single-Page Article Viewing](#)

Share

[Facebook](#)

[Twitter](#)

[Legal Disclaimer](#), [Privacy Policy](#) | [Contact](#)

Copyright © 2004 - 2021 by **Phoronix Media**.

All trademarks used are properties of their respective owners. All rights reserved.