RLBox: Retrofitting Fine Grain Isolation in the Firefox Renderer

UC San Diego
TEXAS
The University of Texas at Austin

Shravan Narayan, Craig Disselkoen, Tal Garfinkel, Sorin Lerner, Hovav Shacham, and Deian Stefan

Motivation

Browsers are important

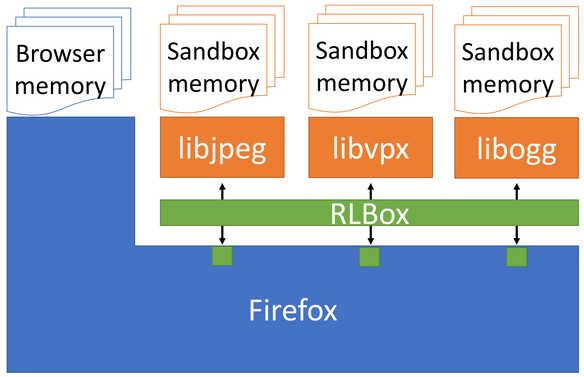
Uses 3rd party libraries

Lib bugs = browsers bugs!

 # CVE-2018-5146: Out of bounds memory write in libvorbis

Reporter	Richard Zhu via Trend Micro's Zero Day Initiative
Impact	critical
Description	

RLBox



A C++ library that:

Abstracts sandbox mechanism: Process, Native Client, Wasm

Mediates app-sandbox comms with APIs & tainted types

RLBox guides changes via compiler errors

```
jpeg_read_header(&img /* ... */);

uint32_t size = img.output_width * img.output_components;

memcpy(outputBuffer, /* ... */, size);
```

```
sandbox.invoke(jpeg_read_header, img /* ... */);

tainted<uint32_t> t_size = img.output_width *  img.output_components;

uint32_t size = t_size.copy_and_verify([](uint32_t val) -> uint32_t {
  assert(val <= outputBufferSize);
  return val;
});

memcpy(outputBuffer, /* ... */,  size);
```

We need fine grain isolation

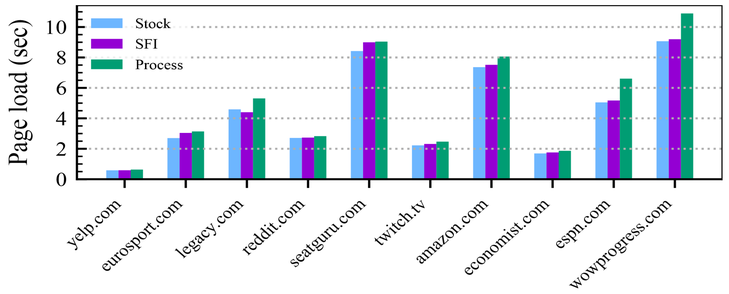
Sandbox 3rd party libraries

libjpeg bug should not compromise Firefox

But sandboxed libs can conduct confused deputy attacks

Evaluation

Sandboxing a lib takes few days
Image: `libjpeg,libpng`
Video: `libtheora,libvpx`
Audio: `libogg`
Compression: `zlib`



RLBox automates 8-64 bounds checks
Manual data validators: 2-51 each 2-4 lines

Ongoing work

RLBox in Firefox from April 2020 on Ubuntu and Mac x64

Sandboxed `libgraphite, libogg, libhunspell` etc.

In progress: sandboxing more libs for more platforms Windows & Android on x32 and ARM.

moz://a HACKS

Securing Firefox with WebAssembly

By Nathan Froyd

Posted on February 25, 2020 in Featured Article, Firefox, Rust, Security, and WebAssembly

Protecting the security and privacy of individuals is a central tenet of Mozilla's mission, and so we constantly endeavor to make our users safer online. With a

So today, we're adding a third approach to our arsenal. RLBox, a new sandboxing technology developed by researchers at the University of California, San Diego, the University of Texas, Austin, and Stanford University, allows us to quickly and efficiently convert existing Firefox components to run inside a