Sydr

Гибридный фаззинг

Андрей Федотов

23 сентября 2022

Sydr: автоматизация поиска и анализа ошибок

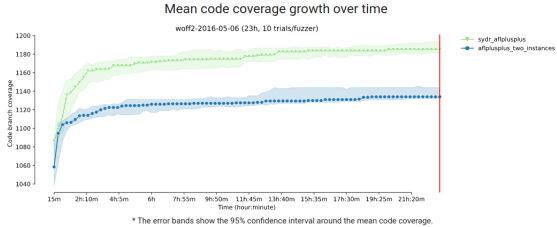
ИСП РАН

Пайплайн динамического анализа:

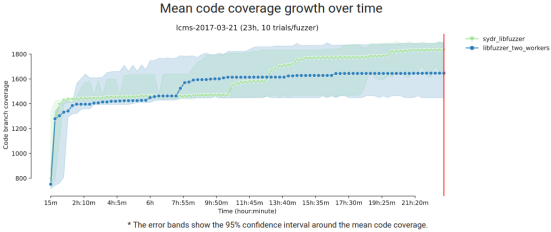
1. sydr-fuzz **run** (запуск фаззинга Sydr&libFuzzer/AFL++)
2. sydr-fuzz **cmin** (минимизация корпуса)
3. sydr-fuzz **cov-*** (сбор покрытия)
4. sydr-fuzz **security** (чекеры)
5. sydr-fuzz **casr** (анализ аварийных завершений)

```
[sydr]
target = "/decode_wav_sydr @@"
jobs = 2

[aflplusplus]
target = "/decode_wav_fuzz"
args = "-x wav.dict -i /corpus"
jobs = 2

[cov]
target = "/decode_wav_cov @@"
```

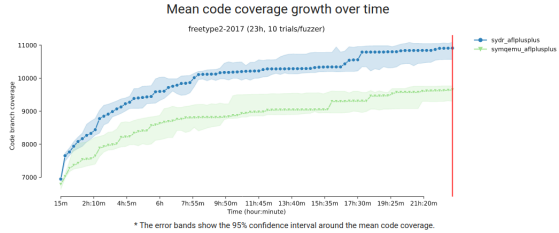
1. Sydr-fuzz достиг большего покрытия, чем другие фаззеры.
2. Sydr-fuzz победил на большем числе бенчмарков.



Sydr+AFLplusplus vs 2xAFLplusplus



Sydr+libFizzer vs 2xlibFuzzer



Sydr+AFLplusplus vs SymQEMU+AFLplusplus

sydr-fuzz.github.io/fuzzbench/

Чекеры находят пропущенные фаззером ошибки

ИСП РАН

github.com/opencv/opencv/issues/22284

opencv/3rdparty/openjpeg/openjp2/image.c:134:

```
l_y1 = p_cp->ty0 + (p_cp->th - 1U) * p_cp->tdy; /* can't overflow */
```

Can't overflow? But we can!

Срабатыване символьного чекера Sydr:

opj_image_comp_header_update:/opencv/3rdparty/openjpeg/openjp2/image.c:134 - imul r15d, eax - **unsigned integer overflow**

Автоматическое подтверждение дефекта санитайзерами:

/opencv/3rdparty/openjpeg/openjp2/image.c:134:40: runtime error: **unsigned integer overflow**: 2 * 4278190076 cannot be represented in type 'unsigned int'

```
Stacktrace:
#0 0x5761e0 in __sanitizer::internal_memmove(...)
                  ....
#7 0xfd5dd4a in vision::image::decode_png(at::Tensor const&, ...)

CrashLine: /torchvision/csrc/io/image/cpu/decode_png.cpp:61
Source:
    58 auto read_callback =
    59     [](png_structp png_ptr, png_bytep output, png_size_t bytes) {
    60       auto reader = static_cast<Reader*>(png_get_io_ptr(png_ptr));
--->61       std::copy(reader->ptr, reader->ptr + bytes, output);
    62       reader->ptr += bytes;
    63     };
CrashSeverity: NOT_EXPLOITABLE SourceAv
```

OSS-Sydr-Fuzz: новые ошибки в открытом ПО

ИСП РАН

github.com/ispras/oss-sydr-fuzz — это форк OSS-Fuzz для гибридного фаззинга с помощью Sydr.

- **30+** проектов и **260+** фаззинг-целей.
- Найдено **80** ошибок в PyTorch, TensorFlow, OpenCV, Torchvision, Tarantool и других проектах.
- Чекеры Sydr помогают находить новые ошибки после фаззинга. Найдено **10+** ошибок с помощью предикатов безопасности.
- Casr существенно сокращает время анализа аварийных завершений (1800+ аварийных завершений свелось к 7 ошибкам в PyTorch).
- Хотите пофаззить open source проект с помощью Sydr? **Ждем Ваших PR!!!**

Группа пользователей Sydr в Telegram: @sydr_fuzz