Поиск уязвимостей с использованием статического анализа кода

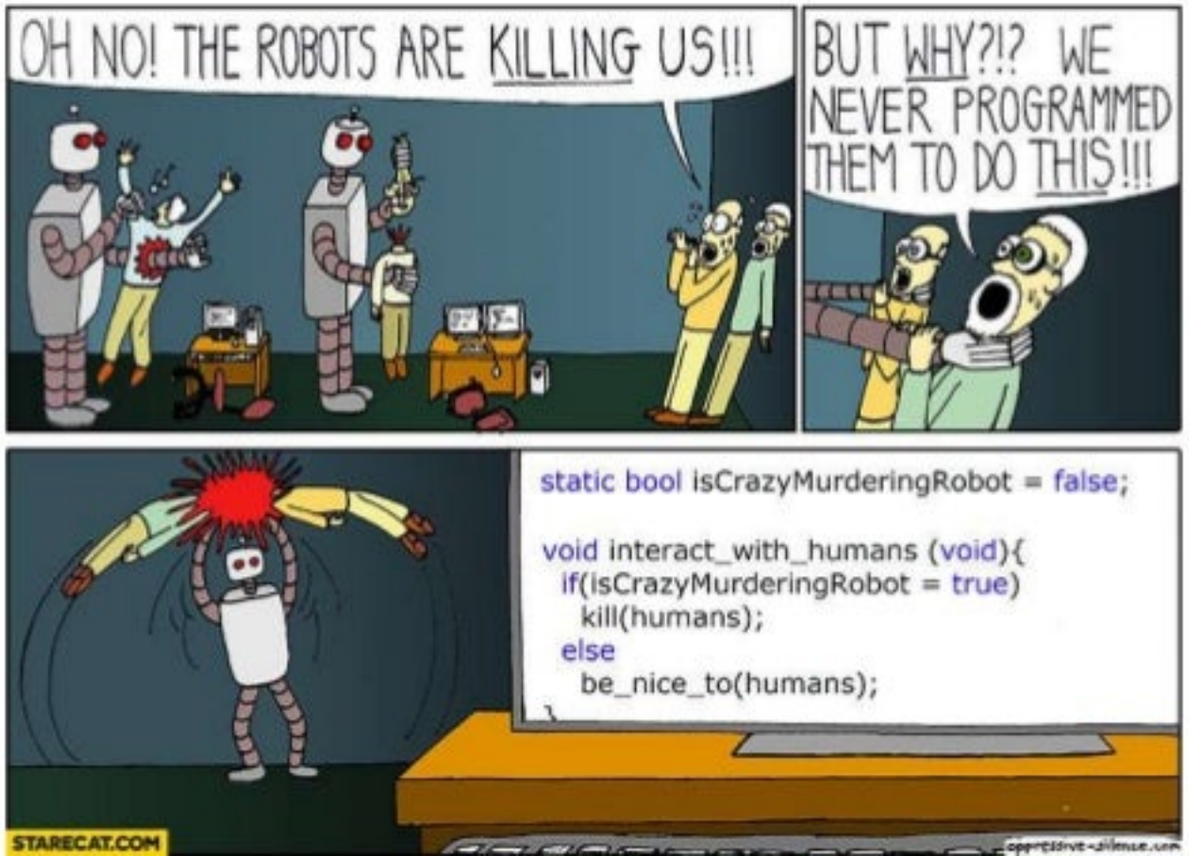
Андрей Карпов
karpov@viva64.com

Евгений Рыжков
evg@viva64.com

www.viva64.com

А оно нам нужно?

- Уязвимости - это те же самые обыкновенные ошибки.
- Зачем их выделять?
- Делайте это, если хотите заработать больше денег.



Аналогия

- Серверы
- Фермы
- Кластеры
- Хранилища
- Скукотища

Облака

- Модно
- Молодёжно
- Престижно

- **Больше платят**

Это и стёб, и не стёб одновременно

- Сейчас лучше быть, например, не админом, а DevOps-специалистом.
- Ещё лучше - SecDevOps!

Поговорим, как стать более ценным ~~программистом~~ экспертом по безопасности

Совсем без скучной терминологии обойтись не получится

- CWE - Common Weakness Enumeration
- CVE - Common Vulnerabilities and Exposures
- Взаимосвязь

Милая ошибка

```
const char *err = strchr(cp, ':')+2;
tor_assert(err);
```

проект Tor

- Проверка, которая ничего не проверяет.
- PVS-Studio: V769 The 'strchr(cp, ':')' pointer in the 'strchr(cp, ':') + 2' expression could be nullptr. In such case, resulting value will be senseless and it should not be used. dns.c 163

Уязвимость

проект illumos-gate

```
char *ptr;
....
ptr = strchr(ptr + 1, '/') + 1;
rw_exit(&sdvp->sdev_contents);
sdev_iter_datasets(dvp, ZFS_IOC_DATASET_LIST_NEXT, ptr);
```

- **CVE-2014-9491**: The devzvol_readdir function in illumos does not check the return value of a strchr call, which allows remote attackers to cause a denial of service (NULL pointer dereference and panic) via unspecified vectors.
- PVS-Studio: V769 The 'strchr(ptr + 1, '/')' pointer in the 'strchr(ptr + 1, '/') + 1' expression could be nullptr. In such case, resulting value will be senseless and it should not be used.

Ошибка (вполне себе кандидат на CVE)

```
char buffer[1001];
int len;
while ((len = pBIO_read(bio, buffer, 1000)) > 0)
{
  buffer[len] = 0;
  fprintf(file, buffer);
}
```

проект WinSCP

- PVS-Studio: V618 It's dangerous to call the 'fprintf' function in such a manner, as the line being passed could contain format specification. The example of the safe code: printf("%s", str); asyncsslsocketlayer.cpp 2247

Уязвимость

```
if (NasConfig.DoDaemon) {    /* daemons use syslog */
  openlog("nas", LOG_PID, LOG_DAEMON);
  syslog(LOG_DEBUG, buf);
  closelog();
} else {
  errfd = stderr;
```

проект Network Audio System

- **CVE-2013-4258**: Format string vulnerability in the osLogMsg function in server/os/aulog.c in Network Audio System (NAS) 1.9.3 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via format string specifiers in unspecified vectors, related to syslog.
- PVS-Studio: V618 It's dangerous to call the 'syslog' function in such a manner, as the line being passed could contain format specification. The example of the safe code: printf("%s", str);

Это не баг, это фича

```
char *str = malloc(vlen + dlen + 1);
memcpy(str, val, vlen);
memcpy(str + vlen, _dexts[i], dlen);
```

проект EFL Core Libraries

- PVS-Studio: V575 The potential null pointer is passed into 'memcpy' function. Inspect the first argument. main.c 112
- В EFL Core Libraries я обнаружил около **700** таких "фич".

По мнению автора Carsten Haitzler, это нормально. Это не ошибки.

Уязвимость

```
vl->data = calloc(vl->size, sizeof(WORD));
temp_word = SwapWord((BYTE*)d, sizeof(WORD));
memcpy(vl->data, &temp_word, vl->size);
```

проект Yerase's TNEF Stream Reader

- **CVE-2017-6298**: An issue was discovered in ytnef before 1.9.1. This is related to a patch described as "1 of 9. Null Pointer Deref / calloc return value not checked."
- PVS-Studio: V575 The potential null pointer is passed into 'memcpy' function. Inspect the first argument.

Не ошибка, а ерунда какая-то

```
u8 other = memcmp(requester->frame_rcvd.iaf.sas_addr,
                  iphy->frame_rcvd.iaf.sas_addr,
                  sizeof(requester->frame_rcvd.iaf.sas_addr));

if (other == 0) {
   ....
}
```

Linux Kernel

- PVS-Studio: V642 Saving the 'memcmp' function result inside the 'unsigned char' type variable is inappropriate. The significant bits could be lost breaking the program's logic. host.c 1789

Уязвимость

проект MySQL

```
typedef char my_bool;
my_bool check_scramble(....)
{
  ....
  return memcmp(hash_stage2, hash_stage2_reassured, SHA1_HASH_SIZE);
}
```

- **CVE-2012-2122**: sql/password.c in Oracle MySQL 5.1.x before 5.1.63, ... , when running in certain environments with certain implementations of the memcmp function, allows remote attackers to bypass authentication by repeatedly authenticating with the same incorrect password, which eventually causes a token comparison to succeed due to an improperly-checked return value.
- PVS-Studio: V642 Saving the 'memcmp' function result inside the 'char' type variable is inappropriate. The significant bits could be lost breaking the program's logic. password.c

Ошибка

```
} else {
  goto no_match; //ATC
  cc = iselCondCode( env, guard );
}
```

проект Valgrind

- V779 Unreachable code detected. It is possible that an error is present. host_arm_isel.c 461

Уязвимость

```
if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
  goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
  goto fail;
  goto fail;
if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
  goto fail;
```

проект iOS

- CVE-2014-1266: The SSLVerifySignedServerKeyExchange function in libsecurity_ssl/lib/sslKeyExchange.c in the Secure Transport feature in the Data Security component in Apple iOS 6.x ..... does not check the signature in a TLS Server Key Exchange message, which allows man-in-the-middle attackers to spoof SSL servers by (1) using an arbitrary private key for the signing step or (2) omitting the signing step.
- V640 The code's operational logic does not correspond with its formatting. The statement is indented to the right, but it is always executed. It is possible that curly brackets are missing.
- V779 Unreachable code detected. It is possible that an error is present

Как видят мир большие боссы

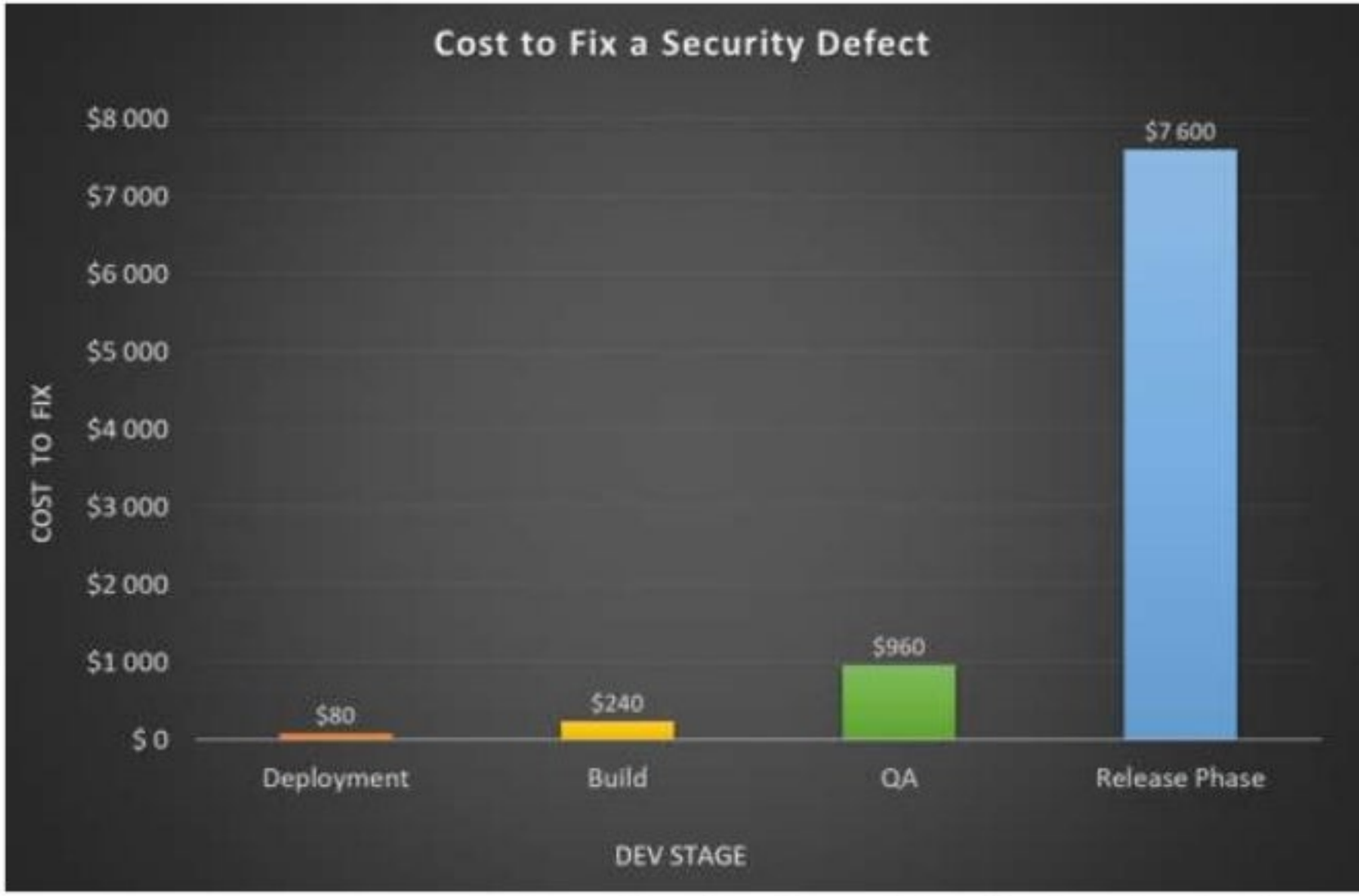
- С точки зрения программиста, ошибки почти не отличаются от потенциальных уязвимостей.
- Зато они отличаются восприятием у непрограммистов.

Ошибка

Уязвимость

Зря паникуем?

- Нет.
- В этом есть смысл.



NIST: National Institute of Standards and Technology

Что делать?

- Объясните, что если будут такие ошибки, этим смогут воспользоваться так-то и так-то:
  - Ненадёжные источники данных
  - Отказ в обслуживании
  - и т.д.

- В общем, те же способы борьбы с ошибками, но используйте другие слова и термины.

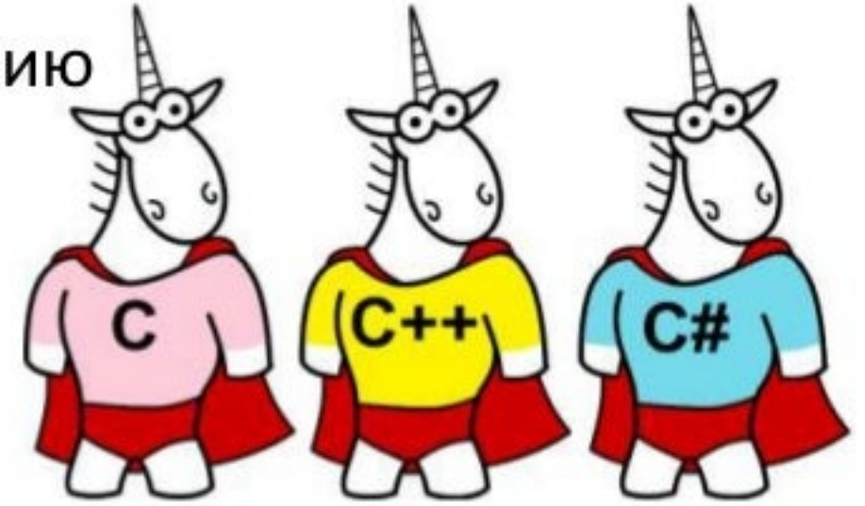
- Инструменты:
  - статические анализаторы
  - динамические анализаторы
  - анализаторы бинарного кода

  - **Теперь с помощью Valgrind вы ищете не утечку памяти, а отказ в обслуживании!**

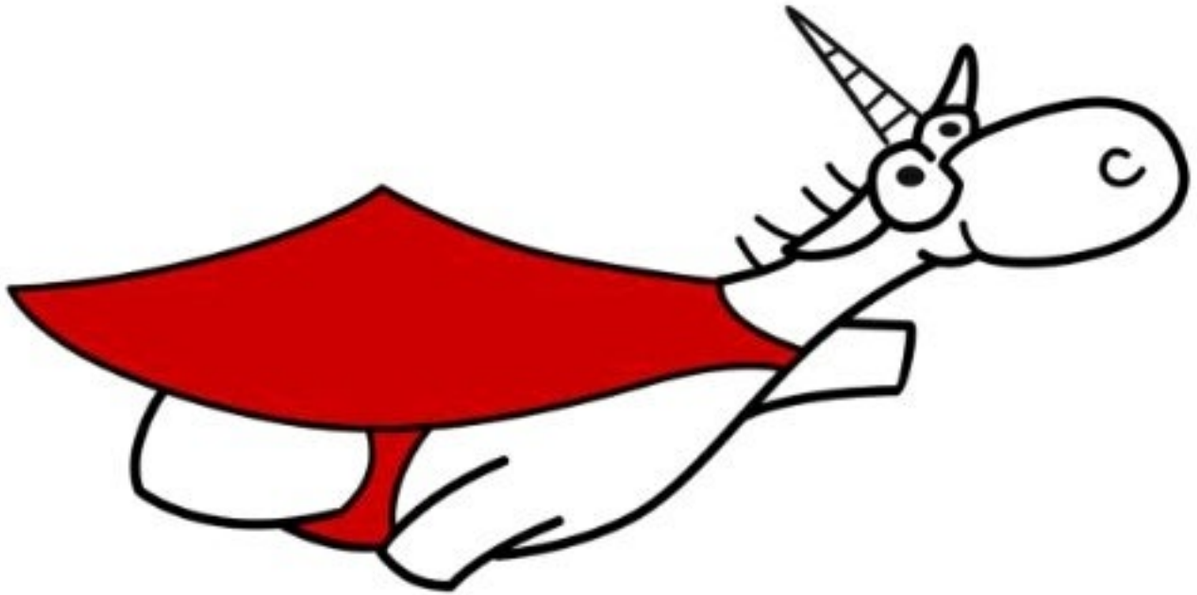
344. Неизвестный художник.
Дай качество! 1931

Наши собственные планы

- Вам мы рассказали, как больше денег заработать
- А мы сами?
- Мы введём в PVS-Studio классификацию ошибок по CWE
- Идеально ещё для рекламы пару уязвимостей найти
- Кто возьмется найти для нас уязвимость?
- Выдаем исследователям бесплатную лицензию



Ответы на вопросы



Андрей Карпов karpov@viva64.com

Евгений Рыжков evg@viva64.com

Сайт PVS-Studio https://www.viva64.com

Twitter @Code_Analysis