

# Практика безопасной разработки средств антивирусной защиты информации как важная составляющая сертификации

Александр Лискин,

Руководитель лаборатории  
антивирусных исследований,  
АО «Лаборатория Касперского»

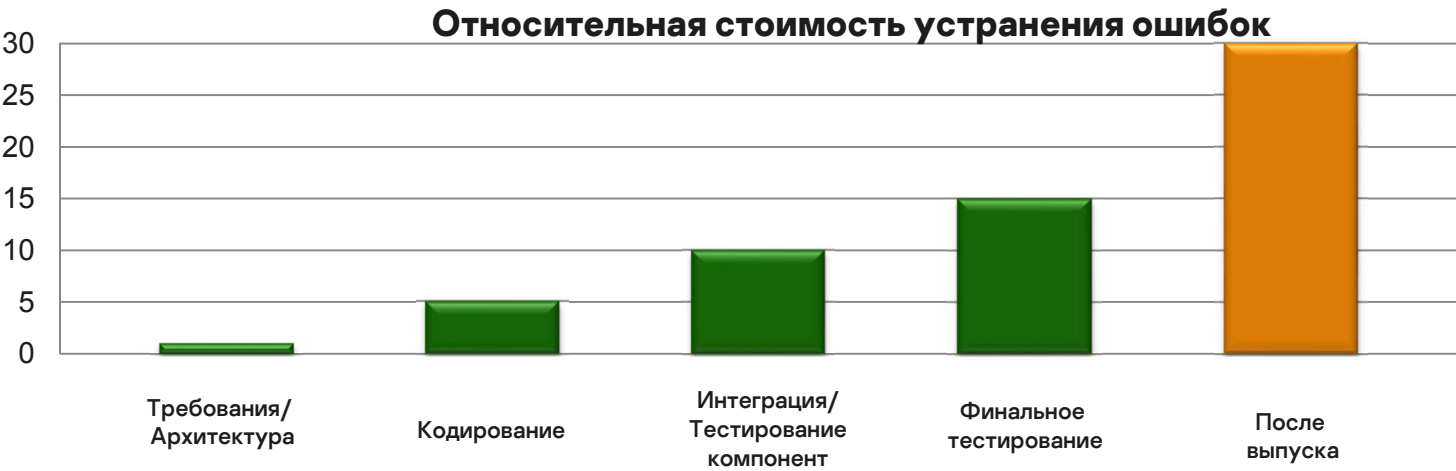
kaspersky

# Agenda

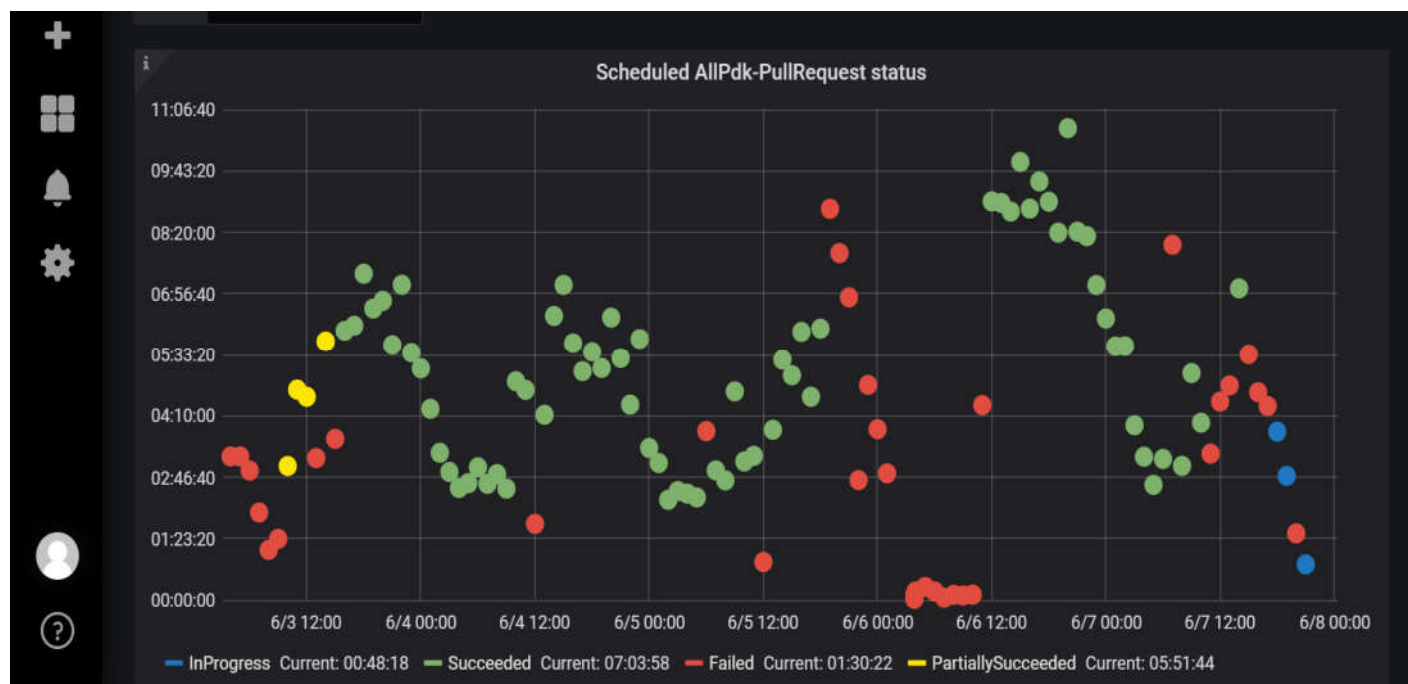
- Что есть безопасная разработка (SDL)
- Структура разработки в АО «Лаборатория Касперского» и с чего начался SDL
- Документы
- Роли
- Процессы и практики, как подружить бумажную и реальную безопасность
- Инструментарий
- Несколько цифр из безопасной разработки

# SDL – цикл безопасной разработки

| 1. TRAINING               | 2. REQUIREMENTS                                  | 3. DESIGN                                    | 4. IMPLEMENTATION             | 5. VERIFICATION                   | 6. RELEASE                           | 7. RESPONSE                    |
|---------------------------|--------------------------------------------------|----------------------------------------------|-------------------------------|-----------------------------------|--------------------------------------|--------------------------------|
| 1. Core Security Training | 2. Establish Security Requirements               | 5. Establish Design Requirements             | 8. Use Approved Tools         | 11. Perform Dynamic Analysis      | 14. Create an Incident Response Plan | Execute Incident Response Plan |
|                           | 3. Create Quality Gates/Bug Bars                 | 6. Perform Attack Surface Analysis/Reduction | 9. Deprecate Unsafe Functions | 12. Perform Fuzz Testing          | 15. Conduct Final Security Review    |                                |
|                           | 4. Perform Security and Privacy Risk Assessments | 7. Use Threat Modeling                       | 10. Perform Static Analysis   | 13. Conduct Attack Surface Review | 16. Certify Release and Archive      |                                |



- **~750 разработчиков**
- **~200k строк кода меняется ежегодно**
- **~70 продуктов (приложений) на поддержке**
- **100+ крупных релизов ежегодно**



**>600 релизов  
в 2019 г.**

---

## Безопасное ПО: с чего начался SDL

6

1. Модели угроз и риски от вирусных аналитиков
  2. Инициатива безопасности от команд и отдельных разработчиков
  3. Зачатки процессов, которые поддерживались изнутри командами разработки
  4. Тестирование
  5. Процедура обработки обращений внешних исследователей
- 
- ▶ Количество известных проблем безопасности на момент старта SDL ~ 115
  - ▶ Проектная команда (частичное вовлечение) сотрудников ~ 7 чел

## Безопасное ПО: с чего начался SDL

7



WikiLeaks

Leaks News About Partners

Search

### Vault 7: CIA Hacking Tools Revealed



Tavis Ormandy

@taviso

Follow

#### Kaspersky "heapgrd" DLL Inject

##### Overview

The Kaspersky AVP.EXE process references a DLL called WHEAPGRD.DLL. 1 by the PSP). Due to a UNICODE/ASCII processing mistake, the DLL name is typically installations, this causes Kaspersky to look for the DLL "CWHEAPGRD process enables us to bypass Kaspersky's protections.

This vulnerability is limited to some of Kaspersky's previous releases (on both )

##### Vulnerable

1. KIS 7
2. KIS 8
3. WKSTN MP3

##### Not Vulnerable

1. KIS 9+
2. WKSTN MP4

Okay, first Kaspersky exploit finished, works great on 15 and 16. Will mail report after dinner. /cc @ryanaraine

| Name              | Private Bytes | Working Set | Session ID | PID                                  |
|-------------------|---------------|-------------|------------|--------------------------------------|
| smss.exe          | 2.0 MB        | 3.0 KB      | 4,000 K    | 11,440 K                             |
| msdnc.exe         | 496.0 KB      | 3,548 K     | 8,068 K    | 2468 Microsoft Distributed Transa... |
| SearchIndexer.exe | 6.8 MB        | 1.3 MB      | 17,720 K   | 13,844 K                             |
| evchost.exe       | 12.9 MB       | 1.9 KB      | 51,476 K   | 22,824 K                             |
| avp.exe           | 0.01          | 212.6 MB    | 85.6 KB    | 209,464 K                            |
| avpui.exe         | 1.09          | 1.3 MB      | 6.2 KB     | 67,932 K                             |
| wmi64.exe         | 140 B         | 20 B        | 1,500 K    | 4,464 K                              |
| calc.exe          |               |             | 388 K      | 148 K                                |
| lsass.exe         | 93.8 KB       | 138.1 KB    | 3,804 K    | 10,168 K                             |
| lsmon.exe         |               |             | 2,544 K    | 4,232 K                              |

7:43 PM - 4 Sep 2015

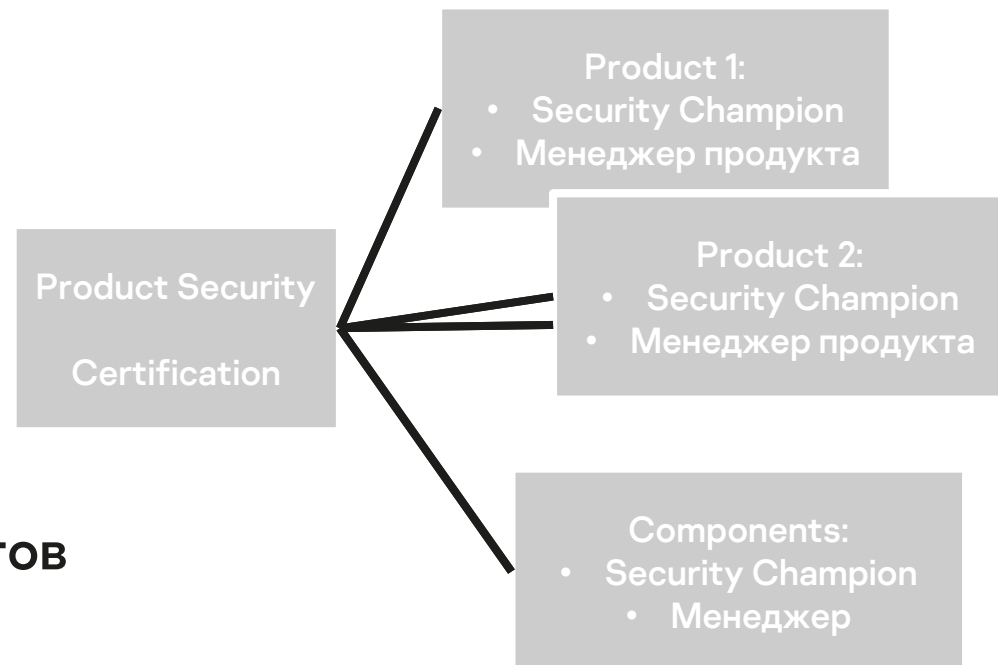
## SDL. Документы

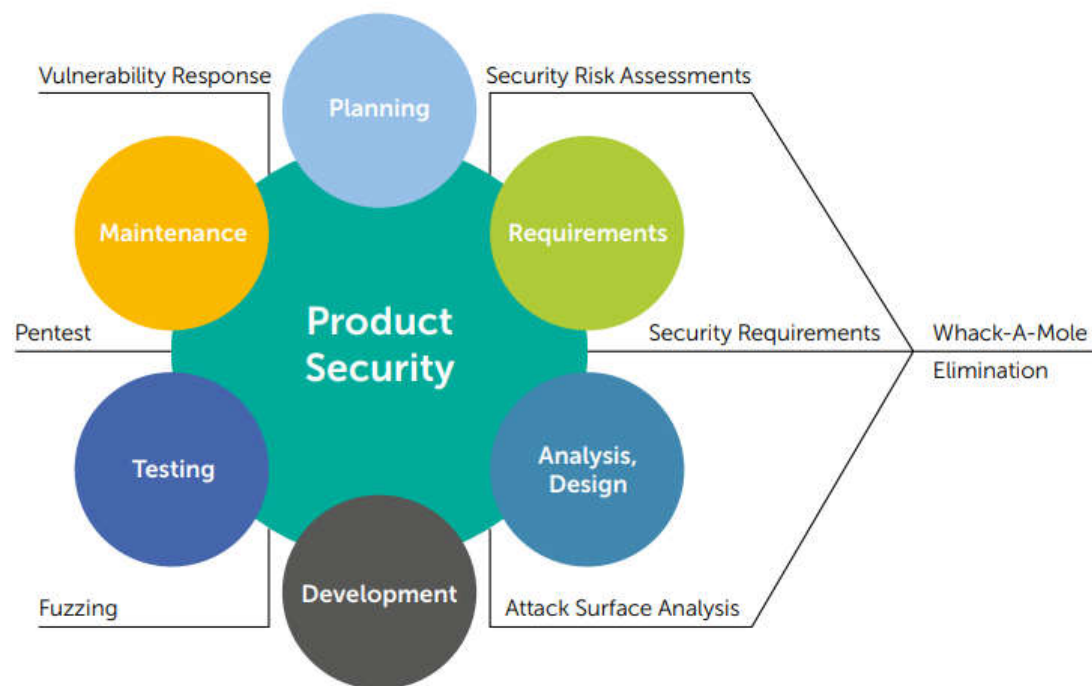
8

| Имя документа                                                                    | Статус      |
|----------------------------------------------------------------------------------|-------------|
| <a href="#">Правила проведения тестирования на проникновение</a>                 | IN PROGRESS |
| <a href="#">Процесс Secure code review</a>                                       | APPROVED    |
| <a href="#">Secure coding guideline (checklist)</a>                              | IN PROGRESS |
| <a href="#">Процесс моделирования угроз</a>                                      | IN PROGRESS |
| <a href="#">Инструкция для Security Champion по процессу моделирования угроз</a> | IN PROGRESS |
| <a href="#">Процесс фаззинг тестирования</a>                                     | IN PROGRESS |
| <a href="#">Процесс управления уязвимостями</a>                                  | IN PROGRESS |
| <a href="#">Руководство по разработке безопасного программного обеспечения</a>   | APPROVED    |
| <a href="#">Процесс статического анализа кода</a>                                | APPROVED    |
| <a href="#">Процесс динамического анализа кода</a>                               | APPROVED    |
| <a href="#">Процесс использования сторонних библиотек</a>                        | APPROVED    |



- **Security чемпионы**
- Менеджеры продуктов
- Команда сертификации
- QA (контроль качества)
- Отдел безопасности продуктов





- **Требования по безопасности**
- **Модели угроз на основании сценариев**
- **Стратегия митигаций рисков**
- **Проверка закрытия рисков**
- **Фаззинг и тестирование на проникновение**
- **Автоматизация тестирования требований**
- **Автоматизация фаззинга**

## SDL. Обучение

11



| Roles                             |                                         |
|-----------------------------------|-----------------------------------------|
| SDL. Вводный курс                 | All                                     |
| Безопасная разработка C/C++       | Developers, Leads, Architects           |
| Моделирование угроз               | PMs, Leads, Architects, sr. Developers. |
| Fuzzing                           | PMs, Leads, Architects, sr. Developers. |
| Безопасность Web приложений       | all                                     |
| Безопасность мобильных приложений | Developers, Leads, Architects           |
| Криптография                      | Leads, Architects, sr. Developers       |

## SDL. VULN. Общие требования

12



| Title                                                  |
|--------------------------------------------------------|
| Up-to-date third party software                        |
| Perform static analysis                                |
| Prevent local privilege escalation                     |
| Mitigate network vulnerabilities (incl OWASP's Top 10) |
| Mitigate risks of sensitive data disclosure            |
| SDL                                                    |
| Basic security requirements                            |
| Secure communication with KL infrastructure            |

## SDL. Моделирование угроз

13



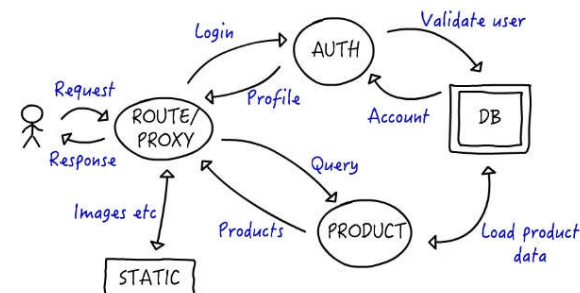
### Методология:

1. STRIDE
2. DREAD
3. PASTA
4. Kill Chain
5. OWASP
6. .... mixed?

### Рекомендации гуру:

1. Концентрироваться на важных продуктах/модулях
2. Описывать и обсуждать изменения
3. Рисовать диаграммы, схемы, идеально – архитектуру (на доске, бумаге, где удобнее)
4. Задавать вопросы «а что если»
5. Идентифицировать риски без привязки к реализации

### Data Flow Diagram



## SDL. Моделирование угроз

14



Отдел безопасности продуктов отвечает за организацию процесса моделирования угроз

**Создание HLA (высокоуровневое описание архитектуры):** Security Champion (команда разработки)

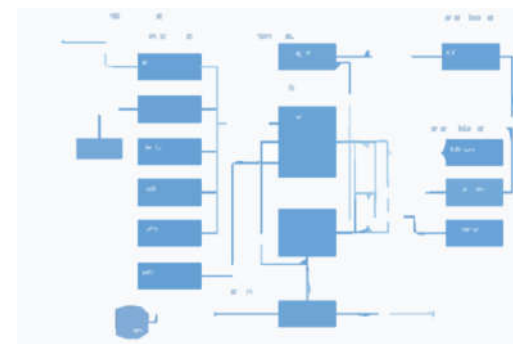
**Описание сценариев, влияющих на безопасность:** Security Champion (команда разработки)

**Создание модели:** отдел безопасности продуктов

**Ревью модели:** архитектор отдела безопасности продуктов

**Основные сценарии, влияющие на безопасность:**

1. Предоставление интерфейса – поверхность атаки
2. Парсинг данных – удаленные атаки с выполнением кода
3. Сетевое взаимодействие – раскрытие данных, перехват управления
4. Изменение окружение – локальное повышение привилегий
5. Хранение данных – раскрытие данных

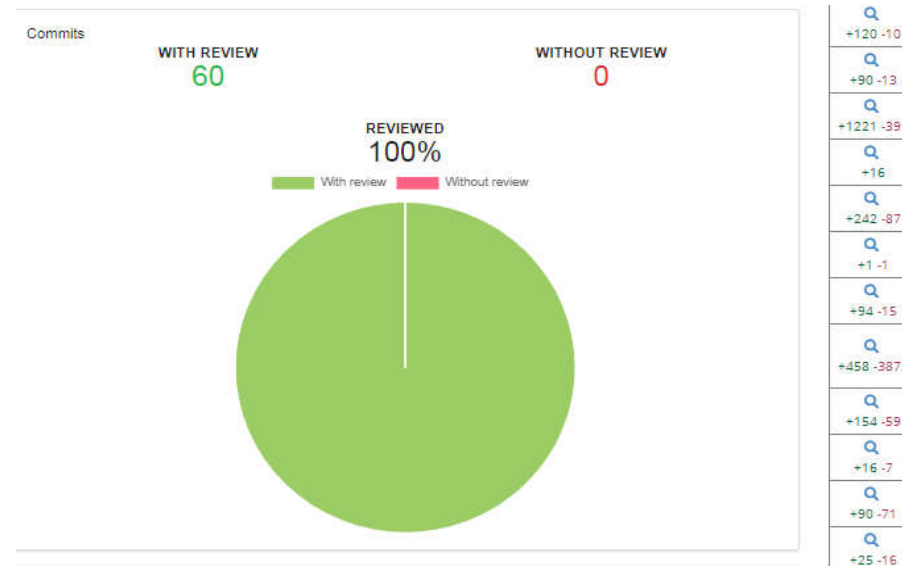


## SDL. Анализ исходного кода

15



Централизованный отчет по покрытию CodeReview  
Сбор артефактов и построение отчетов роботами



## SDL. Статический анализ

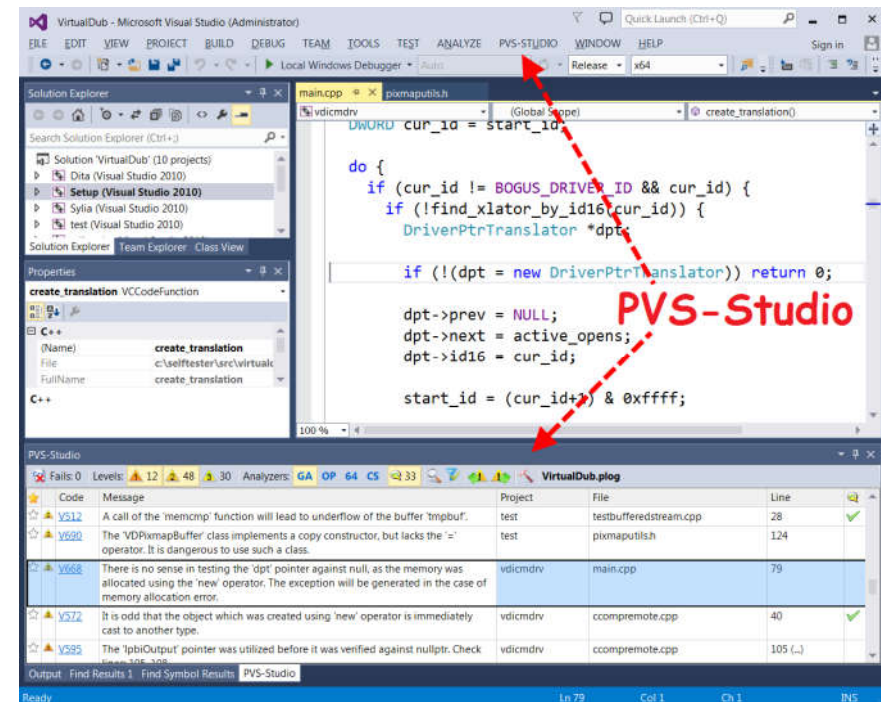
16



### Инструменты:

- PVS Studio
- Clang
- PMD (android)
- Lint (android)

Статический анализатор должен быть в блокирующем режиме





## SDL. 3-rd party библиотеки

17



### Процессы:

1. Ежедневная проверка публичных уязвимостей
2. Приоритезация
3. Передача багов в продукты и компоненты

Продукты, компоненты, сервисы:  
Устранение багов

## 3-rd party libraries

18



### Статистика:

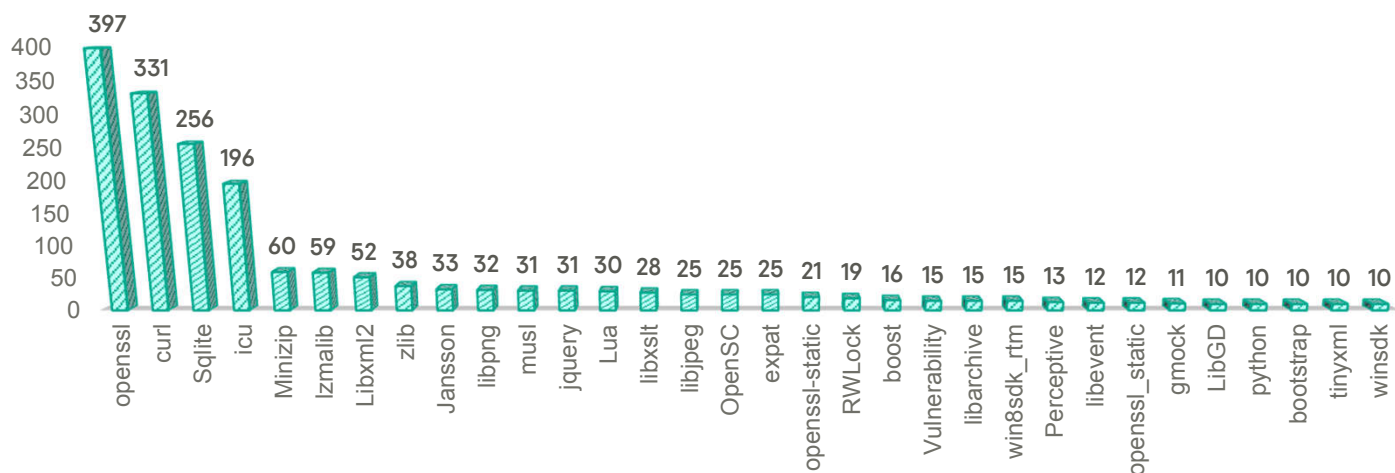
2090+ багов заведено

1800+ багов закрыто

190+ библиотек на поддержке

2000+ библиотек заявлено

## 3RD PARTY: БИБЛИОТЕКИ С 10+ БАГОВ



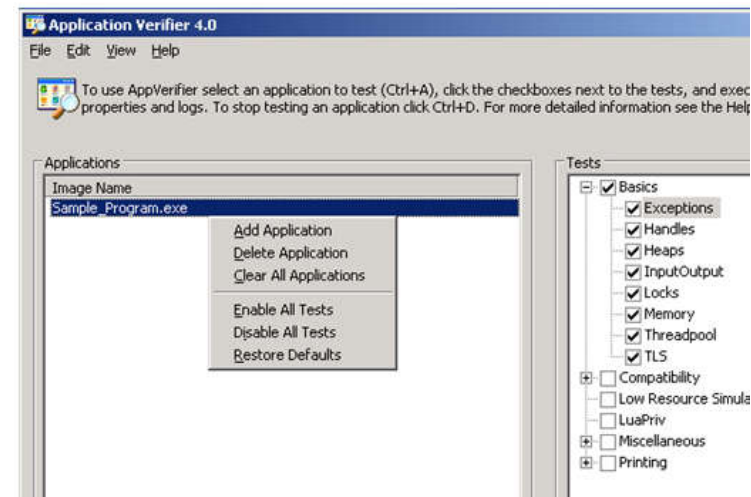
## SDL. Динамический анализ

19



### Инструменты:

- Application Verifier
- Driver Verifier
- Dr.Memory/compiler specific





### Product Security Requirement Verifier

#### DLL Hijacking:

- DLL is loaded by short or invalid path
- DLL is loaded by unsafe path
- Resource is accessed by path with weak ACL

#### Data corruption:

- Write to external folder under privileged user

#### Проверка заголовка исполняемого файла:

- DLL does not support DEP
- DLL does not support ASLR
- DLL does not support isolation
- DLL does not support GS

#### Прочее:

- Write & Execute memory detected
- Using insecure protocol detected
- In process loaded unsigned module



- Добавлены модули парсинга для ряд продуктов
- Пересобраны тулчейны для сборки фаззинг тестов
- Web API для передачи тестов на тестирование
- Новый Web для контроля статусов фазинг-тестов
- Автоматический запуск нового фазинг-теста на ферме



```

=====
==16345== ERROR: AddressSanitizer: unknown-crash on address 0x60820001220b at pc 0x7f4a98de23f7 bp 0x7fffa0b72380 sp 0x7fffa0b71b40
READ of size 25600 at 0x60820001220b thread T0
#0 0x7f4a98de23f6 (/usr/lib/x86_64-linux-gnu/libasan.so.0+0xe3f6)
#1 0x410dad in memcpy /usr/include/x86_64-linux-gnu/bits/string3.h:51
#2 0x410dad in process_heartbeat /home/shadowword/HEARTBLEED/openssl-1.0.1f/selftls+0x40299c
#3 0x49d16c in main /home/shadowword/HEARTBLEED/openssl-1.0.1f/selftls.c:92
#4 0x4a0ca3 in _start (/lib/x86_64-linux-gnu/libc.so.6+0x21ec4)
#5 0x465a2d in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21ec4)
#6 0x4764b3 in _start (/lib/x86_64-linux-gnu/libc.so.6+0x21ec4)
#7 0x402487 in main /home/shadowword/HEARTBLEED/openssl-1.0.1f/selftls.c:92
#8 0x7f4a9882cec4 (/lib/x86_64-linux-gnu/libc.so.6+0x21ec4)
#9 0x40299c in _start (/home/shadowword/HEARTBLEED/openssl-1.0.1f/selftls+0x40299c)
0x608200016748 is located 0 bytes to the right of 17736-byte region [0x608200012200,0x608200016748)
allocated by thread T0 here:
#0 0x7f4a98de941a (/usr/lib/x86_64-linux-gnu/libasan.so.0+0x1541a)
#1 0x4d7946 in CRYPTO_malloc /home/shadowword/HEARTBLEED/openssl-1.0.1f/crypto/mem.c:308
  
```

# Fuzzing with AFL

## SDL. Fuzzing

22



|                       |             |                                          |        |     |   |   |
|-----------------------|-------------|------------------------------------------|--------|-----|---|---|
| STATISTICS            | 26 Finished | ▼ KSVLA                                  | KSV LA |     |   |   |
| Fuzzing statistics    | 13 Finished | ➤ KSVLA_6/28/2019 1:28:35 PM             | KSV LA |     |   |   |
| All running builds    | 13 Finished | ▼ KSVLA_6/28/2019 2:59:16 PM             | KSV LA |     |   |   |
| All builds with crash | Finished    | viis_client_HostInfo                     | KSV LA | 94% | 1 | 2 |
| All queued builds     | Finished    | viis_client_InfrastructureItem           | KSV LA | 96% | 0 | 4 |
| INFORMATION           | Finished    | viis_client_InfrastructureItems          | KSV LA | 96% | 0 | 0 |
| Fuzzing API Doc       | Finished    | viis_client_InfrastructureWarnings       | KSV LA | 96% | 1 | 2 |
| Get Risk Area Path    | Finished    | viis_client_InventoryItems               | KSV LA | 97% | 1 | 2 |
|                       | Finished    | viis_client_InventoryItemsActions        | KSV LA | 93% | 2 | 4 |
|                       | Finished    | viis_client_removedKeys                  | KSV LA | 87% | 3 | 3 |
|                       | Finished    | viis_client_ViisAccountInfo              | KSV LA | 87% | 0 | 0 |
|                       | Finished    | viis_client_ViisApiInfo                  | KSV LA | 91% | 0 | 0 |
|                       | Finished    | viis_client_ViisBoardRecord              | KSV LA | 96% | 1 | 0 |
|                       | Finished    | viis_client_ViisGeneratedCertificateInfo | KSV LA | 91% | 0 | 4 |
|                       | Finished    | viis_client_ViisNsxInfo                  | KSV LA | 90% | 0 | 0 |
|                       | Finished    | viis_client_ViisServiceInfo              | KSV LA | 97% | 1 | 2 |

## SDL. Публичные уязвимости

23



### Обратная связь:

☐ Почтовый ящик

[Vulnerability@kaspersky.com](mailto:Vulnerability@kaspersky.com)

☐ Форум [support.kaspersky.ru](http://support.kaspersky.ru)

☐ Web-Форма обратной связи

☐ Площадка HackerOne

The screenshot shows the HackerOne interface for Kaspersky Lab. At the top, there's a breadcrumb trail: 'Начало → Поддержка → Отчет по уязвимостям'. Below this is a sidebar with a purple 'Все продукты' button and a blue 'Сообщить нам' button. The main content area is titled 'Отчет по уязвимостям: Сообщить нам' and contains the text: 'Политика «Лаборатории Касперского» в отношении сообщений об уязвимостях и информации об уязвимостях. Мы признательны исследователям в области безопасности за их важную деятельность по обнаружению потенциальных уязвимостей в наших продуктах, а также за сообщения о них в «Лабораторию Касперского».' Below this is the Kaspersky Lab logo and a description: 'Kaspersky Lab is the world's largest privately held vendor of Internet security solutions for businesses and consumers.' At the bottom, there's a navigation bar with links: Policy, Hacktivity, Thanks, Updates (0), Insights, and a green 'Submit Report' button.

## SDL. Публичные уязвимости

24



The screenshot shows the Kaspersky Lab website's 'Vulnerability Report' section. The header includes the Kaspersky logo and navigation links like 'SOLUTIONS', 'RENEW', 'DOWNLOADS', 'SUPPORT', 'RESOURCE CENTER', 'PARTNERS', and 'ABOUT'. The main content area is titled 'Vulnerability Report: List of Advisories'. It features a sidebar with 'Product Select' and a list of links: 'Overview', 'Report a vulnerability', and 'List of Advisories'. The main text area contains the 'Kaspersky Lab Policy on Vulnerability Reporting and Disclosure', which states that Kaspersky Lab appreciates security researchers and provides a form for reporting vulnerabilities. It also includes a link to the 'Vulnerability report form' and a feedback section asking 'Was this information helpful?' with 'Yes' and 'No' buttons. On the right, there is a list of advisories with dates and expand/collapse icons.

**Vulnerability Report: List of Advisories**

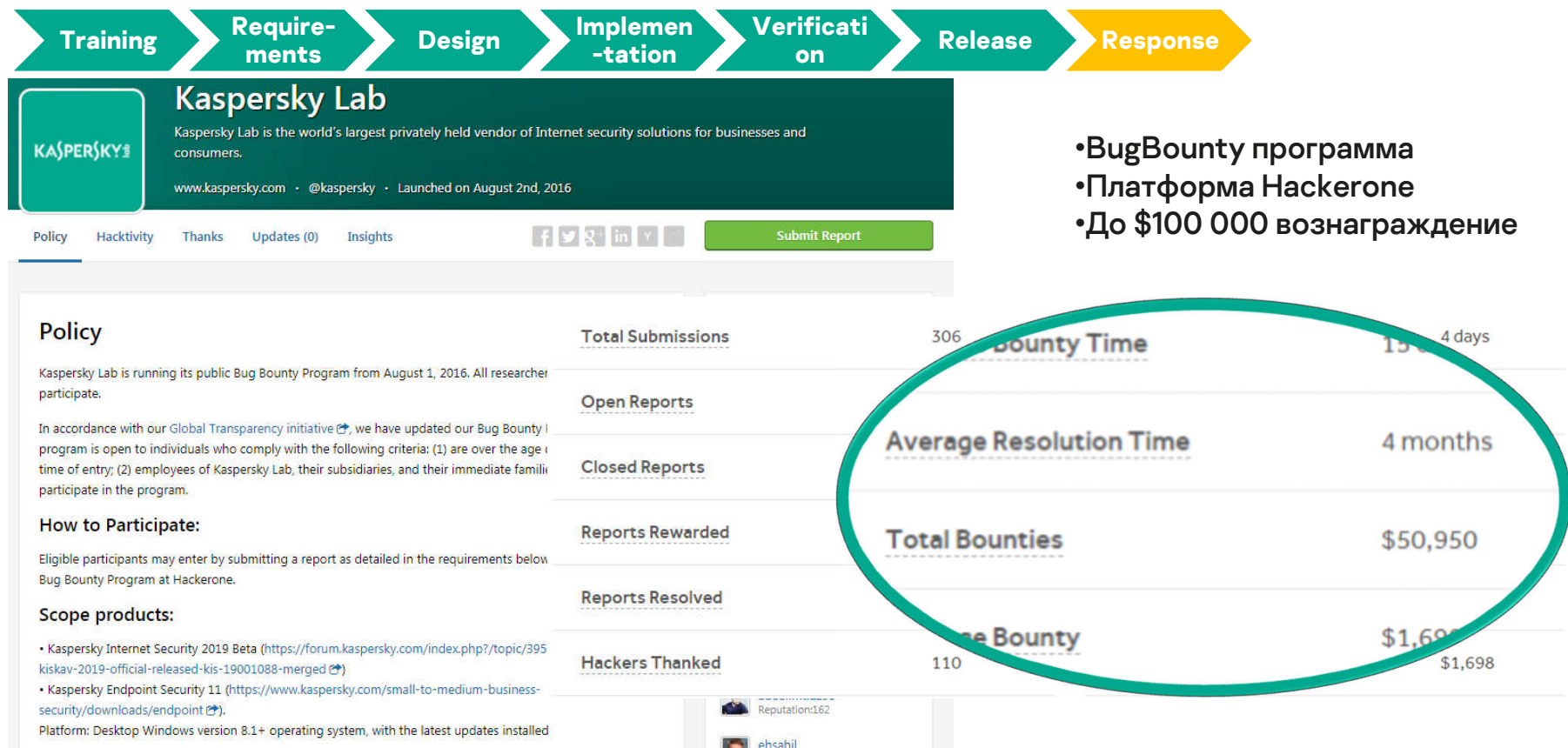
Kaspersky appreciates the ongoing efforts of the independent researchers that help us make our products and solutions more efficient and better protected. Below you can find a list of disclosed vulnerabilities and researchers that reported them to us.

- [Advisory issued on 11th July, 2019](#) +
- [Advisory issued on 8th July, 2019](#) +
- [Advisory issued on 8th May, 2019](#) +
- [Advisory issued on 24th December, 2018](#) +
- [Advisory issued on 19th July, 2018](#) +
- [Advisory issued on 12th April, 2018](#) +



## SDL. Публичные уязвимости

25



- BugBounty программа
- Платформа Hackerone
- До \$100 000 вознаграждение

## SDL. Публичные уязвимости

26



Advisory issued on 8th May, 2019

### Description

Kaspersky Lab has fixed a security issue [CVE-2019-8285](#) in its products that could potentially allow third-parties to remotely execute arbitrary code on a user's PC with system privileges. The security fix was deployed to Kaspersky Lab customers on 4th April, 2019 through a product update.

This issue was classified as heap-based buffer overflow vulnerability. Memory corruption during JS file scan could lead to execution of arbitrary code on a user machine.

CVSSv3 Score: 8.0

CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H

### List of affected products

Kaspersky Lab products with antivirus databases.

### Fixed Versions

Kaspersky Lab products with antivirus databases released after 4th April, 2019.

### Acknowledgments

We would like to thank researchers from the Imagin

1

#548737

Remote code execution

State ☒ Resolved (Closed)

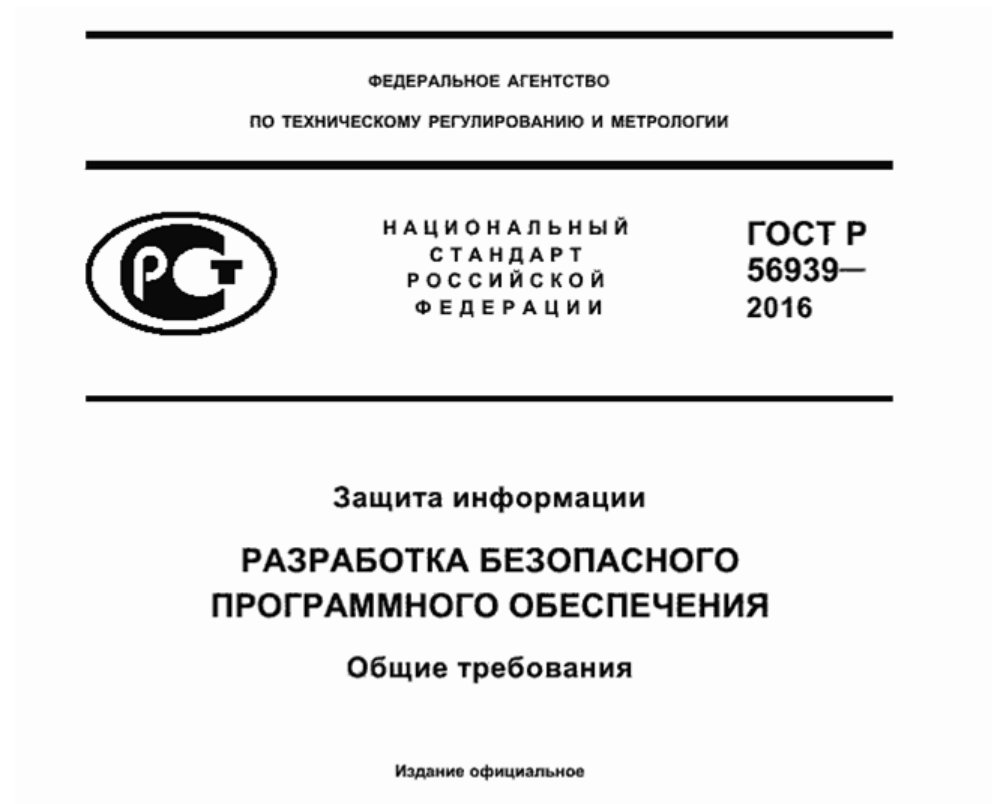
Reported To Kaspersky

Asset Add

References Edit

Weakness [Heap Overflow](#)  
Edit

Bounty \$23,000



# Спасибо!

Александр Лискин

Руководитель лаборатории антивирусных исследований,  
АО «Лаборатория Касперского»

kaspersky