Практика безопасной разработки средств антивирусной защиты информации как важная составляющая сертификации

Александр Лискин,

Руководитель лаборатории
антивирусных исследований,
АО «Лаборатория Касперского»

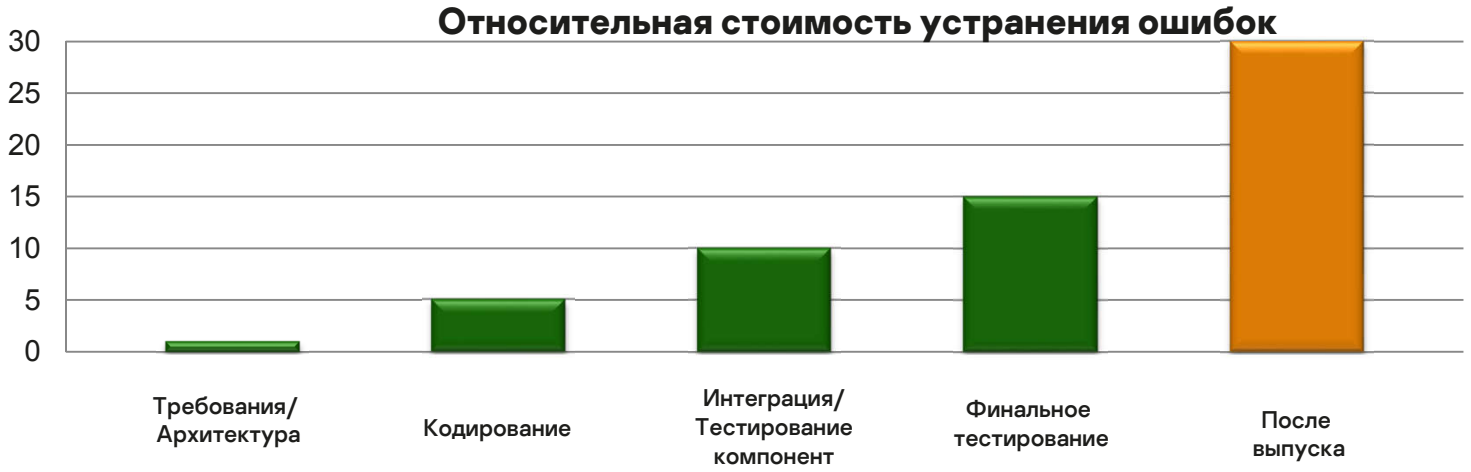
kaspersky

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

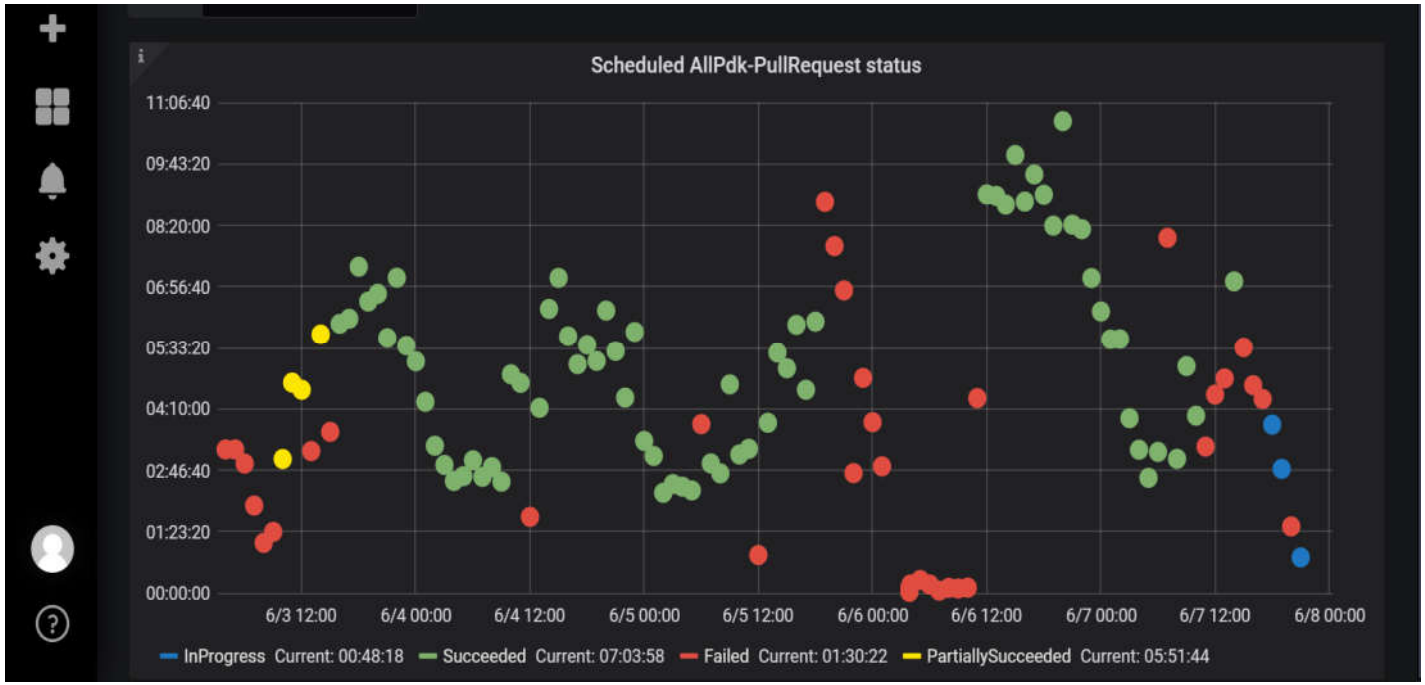
SDL – цикл безопасной разработки

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

Разработка в ЛК: цифры



>600 релизов в 2019 г.

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

WikiLeaks Leaks News About Partners Search

Vault 7: CIA Hacking Tools Revealed

Kaspersky "heapgrd" DLL Inject

Overview

The Kaspersky AVP.EXE process references a DLL called WHEAPGRD.DLL. T
by the PSP). Due to a UNICODE/ASCII processing mistake, the DLL name is p
typicall 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)

Vunerable

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

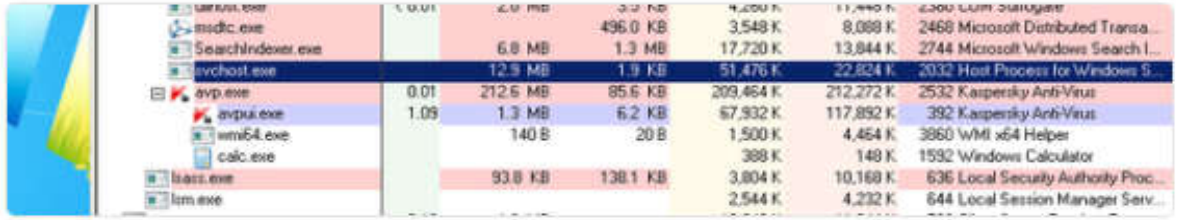
Not Vulnerable

1. KIS 9+
2. WKSTN MP4

Tavis Ormandy
@taviso

Follow

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

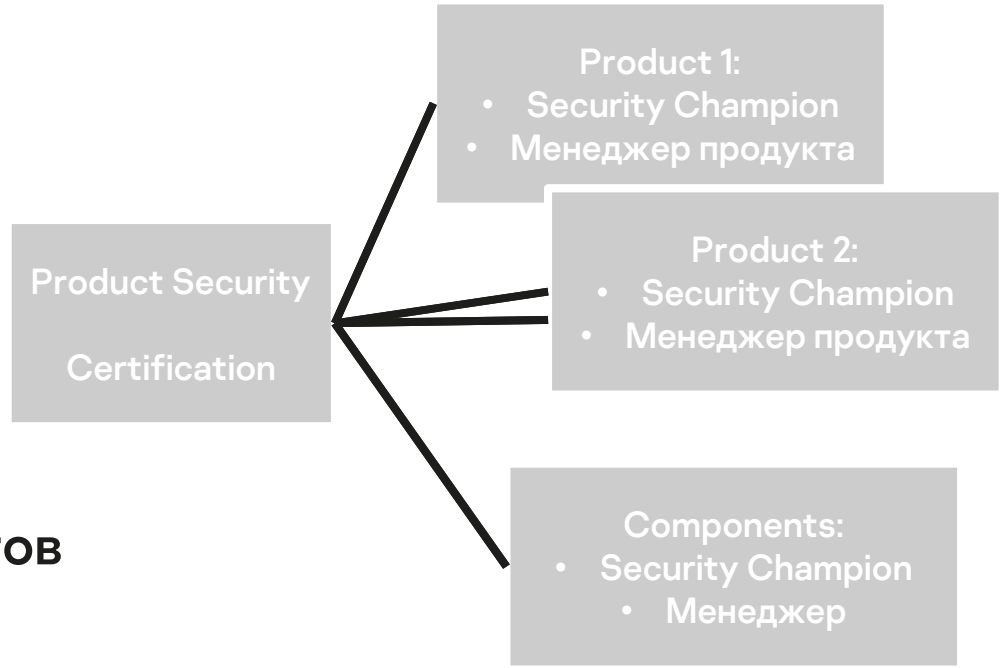


7:43 PM - 4 Sep 2015

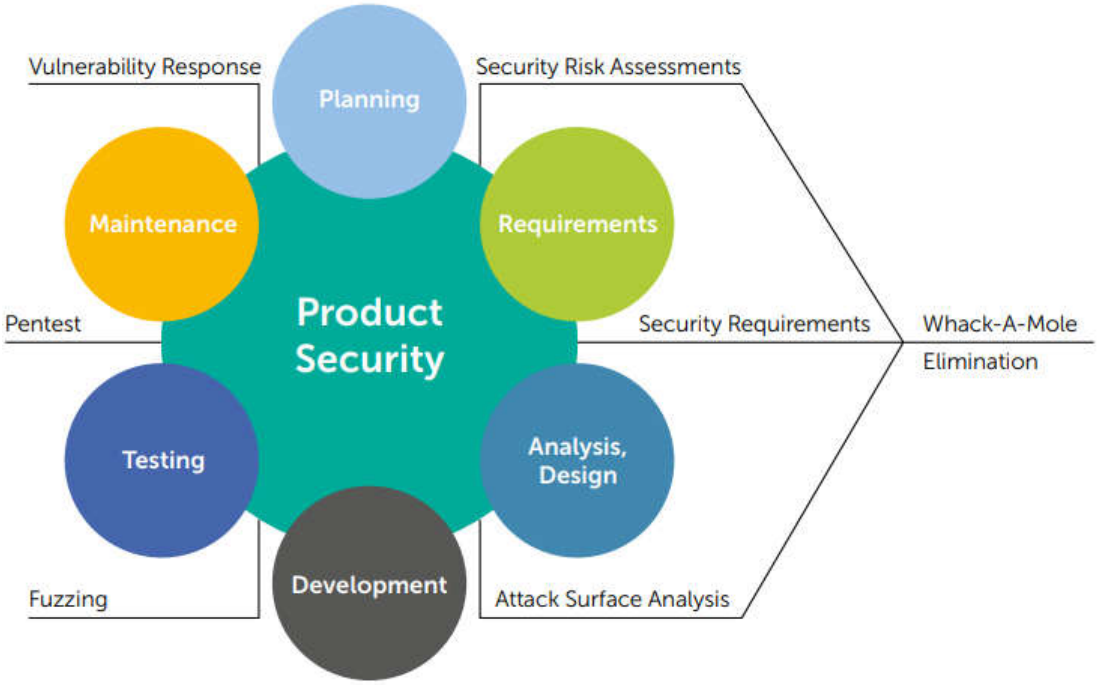
SDL. Документы

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

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



Отдел безопасности ПО



- **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

	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

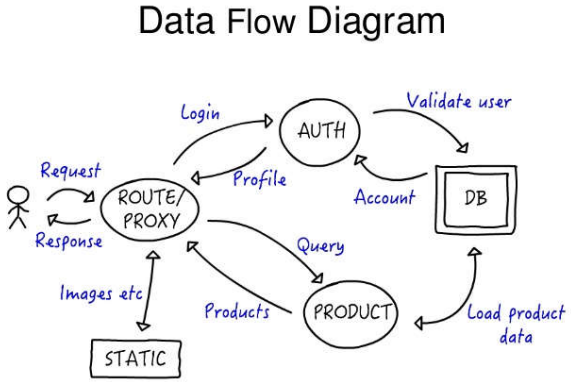
Title
Up-to-date third party software
Perform static analysis
Prevent local privilege escalation
Mitigate network vulnerabilities (incl OWASP's Top 10)
Mitigate risks of sensitive data disclosure
SDL
Basic security requirements
Secure communication with KL infrastructure

SDL. Моделирование угроз

Training | Require-ments | **Design** | Implemen-tation | Verificati on | Release | Response

Методология:

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



Рекомендации гуру:

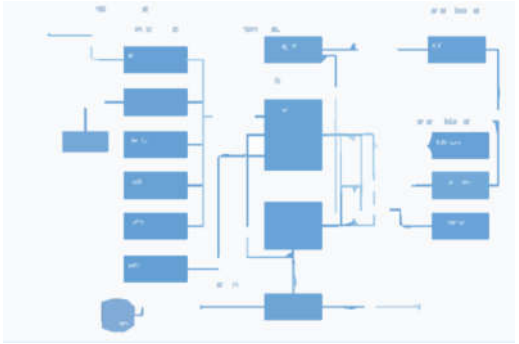
1. Концентрироваться на важных продуктах/модулях
2. Описывать и обсуждать изменения
3. Рисовать диаграммы, схемы, идеально – архитектуру (на доске, бумаге, где удобнее)
4. Задавать вопросы «а что если»
5. Идентифицировать риски без привязки к реализации

SDL. Моделирование угроз

Training | Require-ments | Design | Impleme n-tation | Verificat ion | Release | Respons e

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



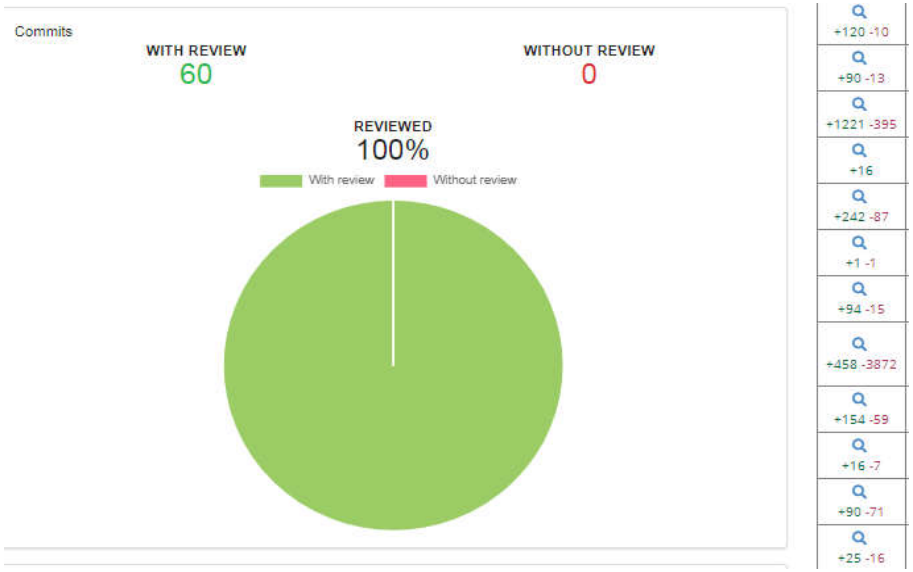
Основные сценарии, влияющие на безопасность:

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

Training | Require-ments | Design | Implemen-tation | Verificati on | Release | Response

Централизованный отчет по покрытию CodeReview
Сбор артефактов и построение отчетов роботами

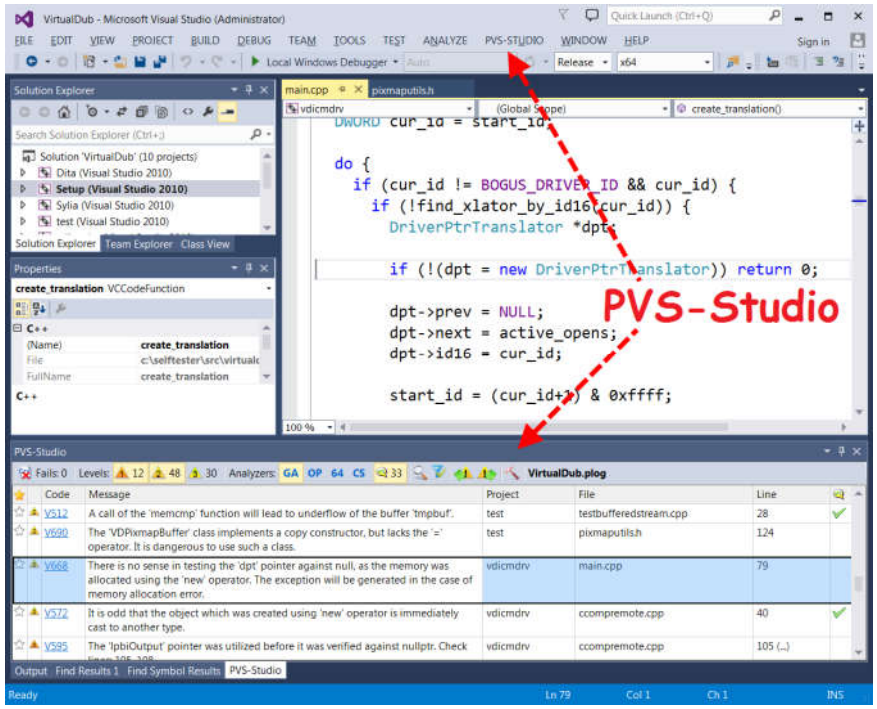


Training | Require-ments | Design | Implemen-tation | Verificati on | Release | Response

Инструменты:

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

Статический анализатор должен быть в **блокирующем режиме**



SDL. 3-rd party библиотеки

Процессы:

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

Продукты, компоненты, сервисы:
Устранение багов

3-rd party libraries

Training | Require-ments | Design | Implemen-tation | Verificati on | Release | Response

Статистика:
2090+ багов заведено
1800+ багов закрыто

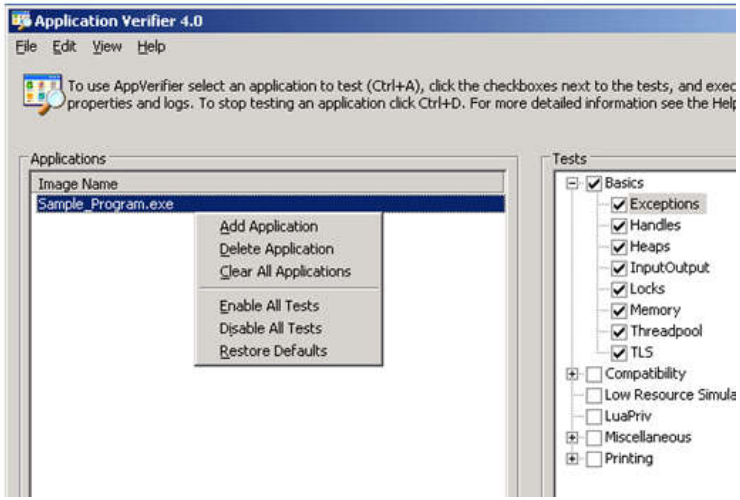
190+ библиотек на поддержке
2000+ библиотек заявлено

SDL. Динамический анализ

Training | Require-ments | Design | Implemen-tation | Verification | Release | Response

Инструменты:

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



SDL. Динамический анализ

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 priveleged 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

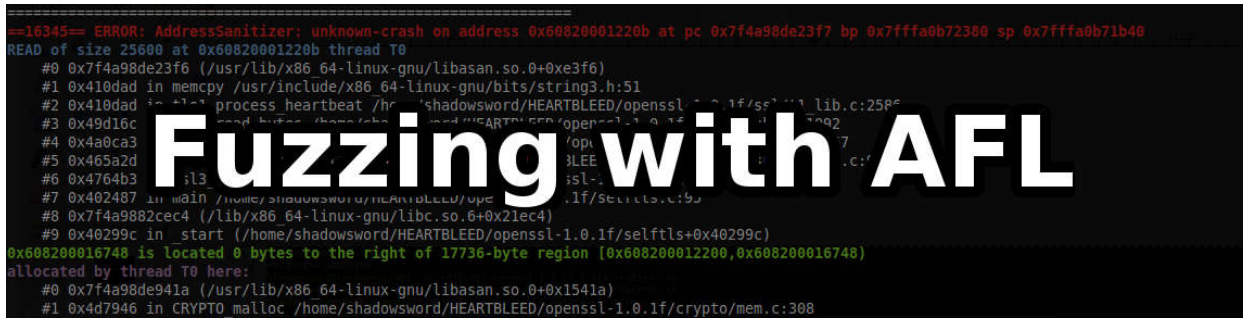
Прочее:

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

SDL. Fuzzing

Training | Require-ments | Design | Implemen-tation | Verificati on | Release | Response

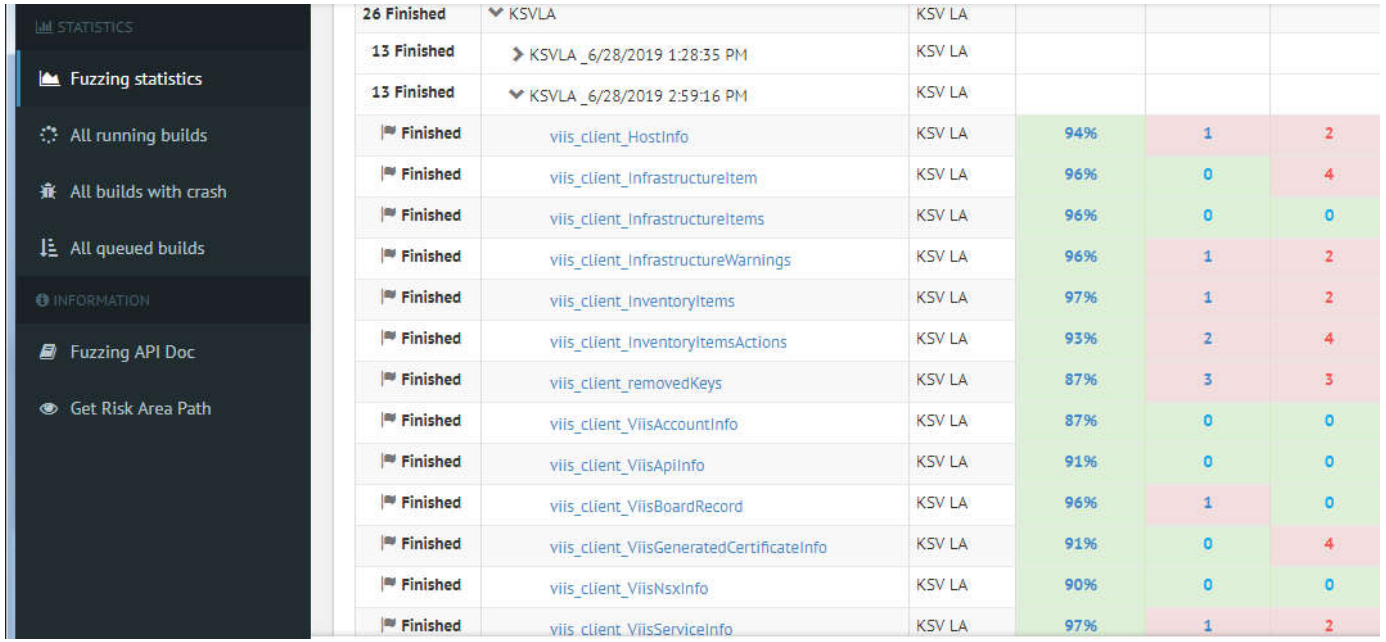
- Добавлены модули парсинга для ряд продуктов
- Пересобраны тулчейны для сборки фаззинг тестов
- Web API для передачи тестов на тестирование
- Новый Web для контроля статусов фазинг-тестов
- Автоматический запуск нового фазинг-теста на ферме



Fuzzing with AFL

SDL. Fuzzing

Training | Require-ments | Design | Implemen-tation | Verification | Release | Response



26 Finished	KSVLA	KSV LA			
13 Finished	KSVLA _6/28/2019 1:28:35 PM	KSV LA			
13 Finished	KSVLA _6/28/2019 2:59:16 PM	KSV LA			
Finished	viis_client_HostInfo	KSV LA	94%	1	2
Finished	viis_client_InfrastructureItem	KSV LA	96%	0	4
Finished	viis_client_InfrastructureItems	KSV LA	96%	0	0
Finished	viis_client_InfrastructureWarnings	KSV LA	96%	1	2
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

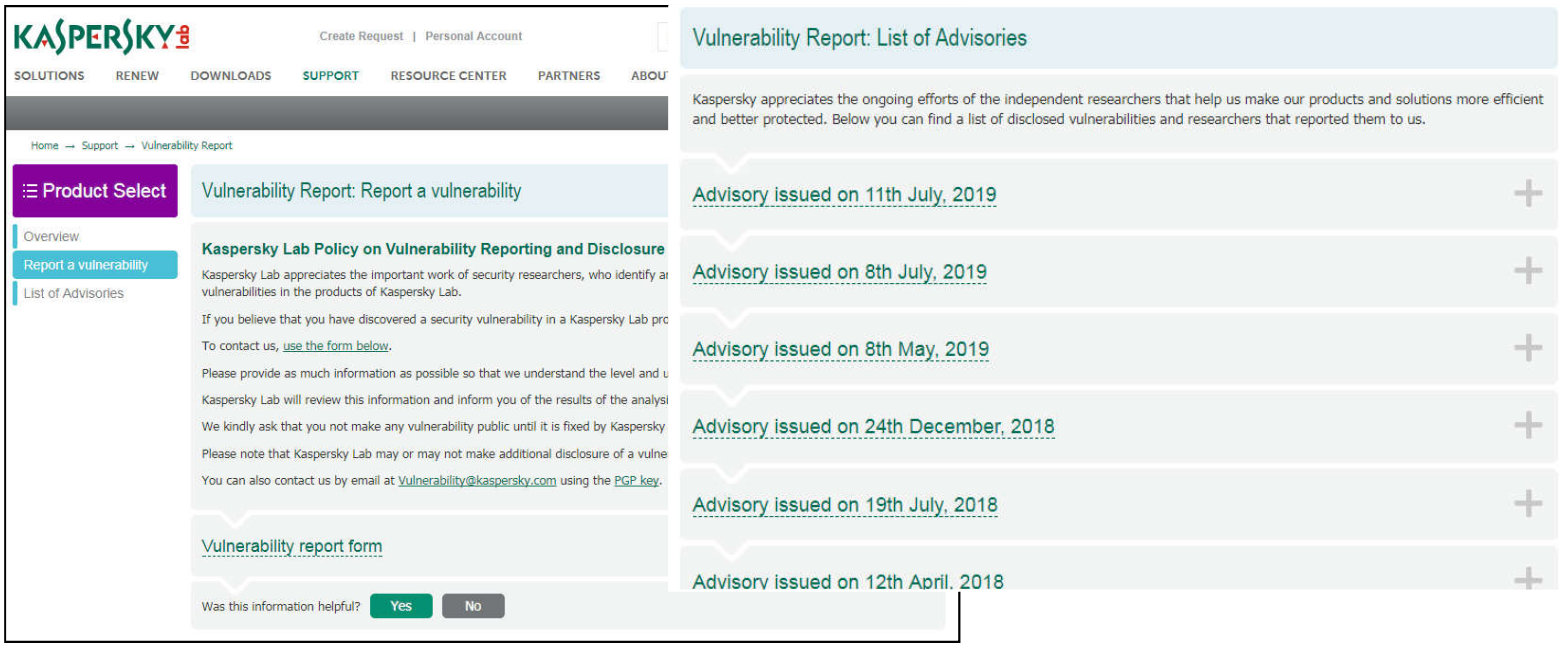
Training | Require-ments | Design | Implemen-tation | Verificati on | Release | Response

Обратная связь:

- ❑ Почтовый ящик Vulnerability@kaspersky.com
- ❑ Форум support.kaspersky.ru
- ❑ Web-Форма обратной связи
- ❑ Площадка HackerOne

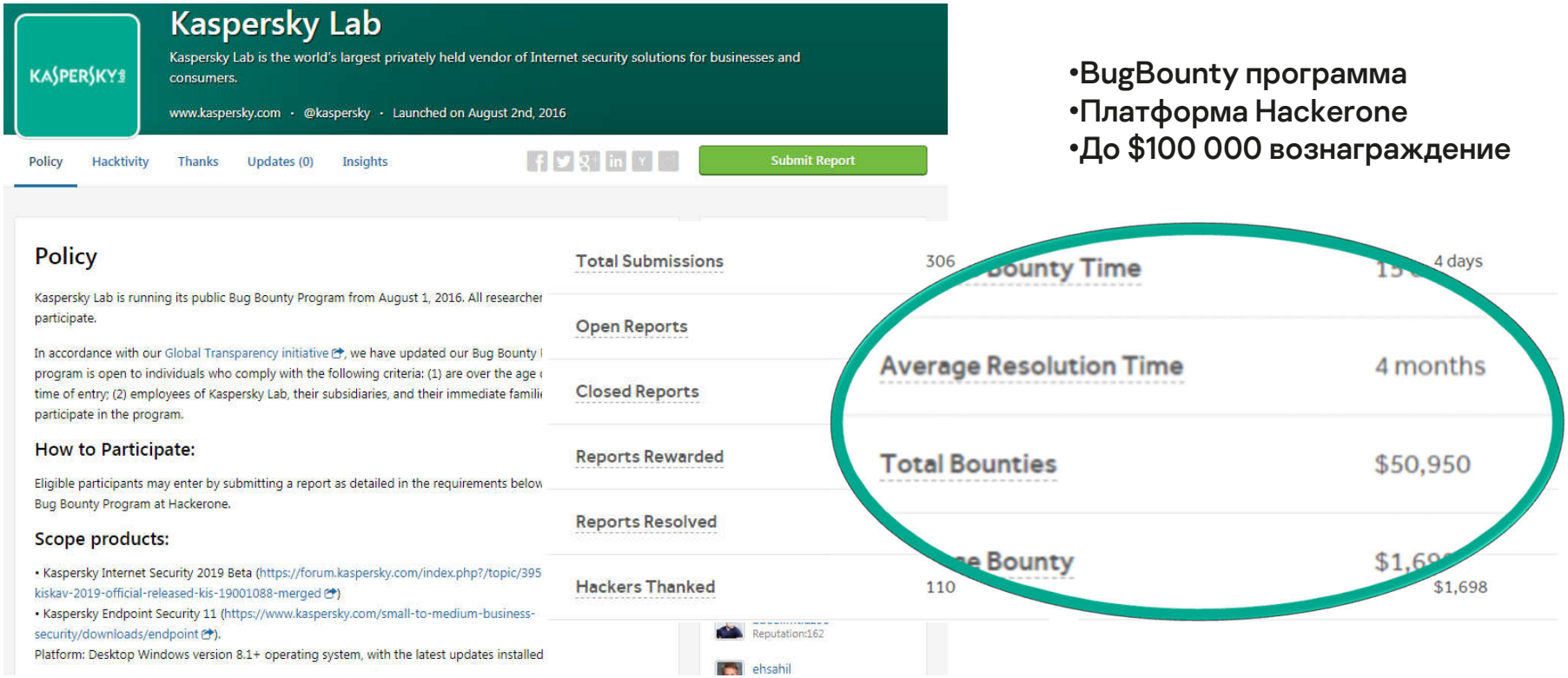
SDL. Публичные уязвимости

Training | Require-ments | Design | Implemen-tation | Verificati on | Release | Response



SDL. Публичные уязвимости

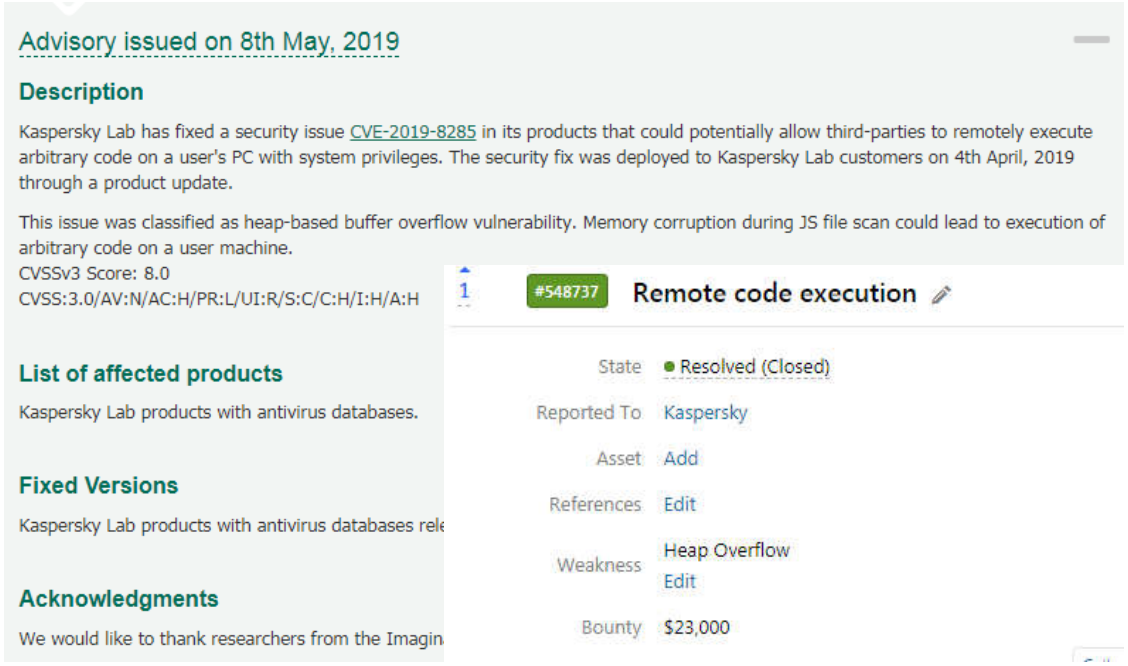
Training | Require-ments | Design | Implemen-tation | Verificati on | Release | Response



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

SDL. Публичные уязвимости

Training | Require-ments | Design | Implemen-tation | Verificati on | Release | Response



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 rele

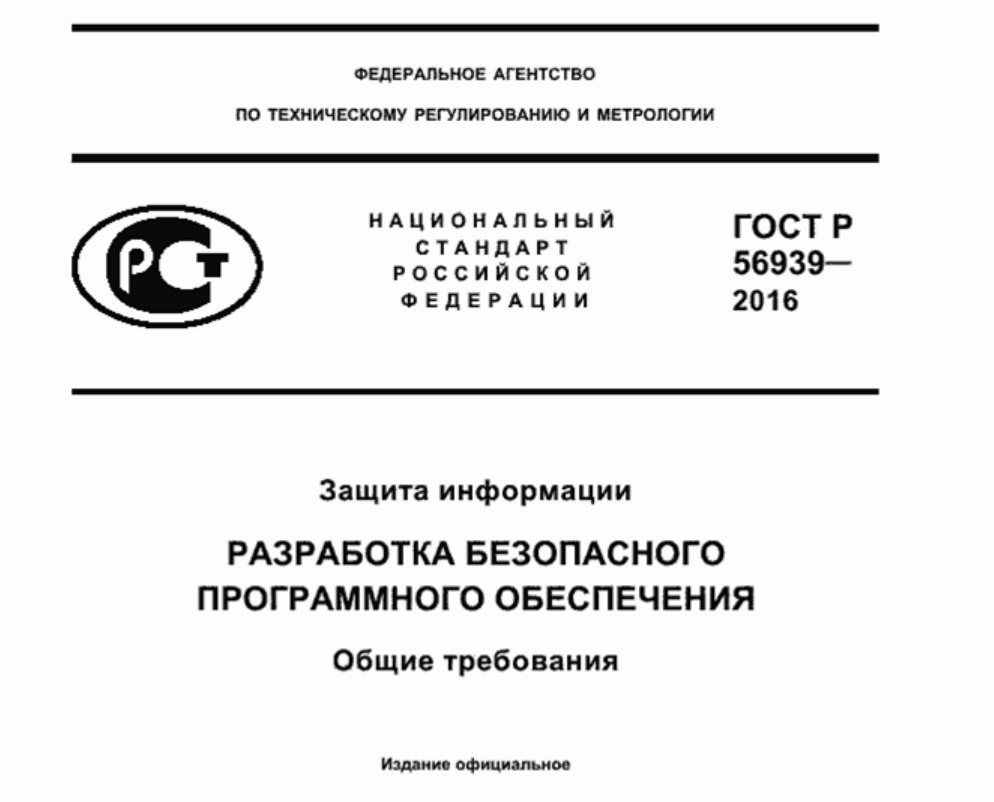
Acknowledgments

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

ГОСТ по безопасной разработке



ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 56939— 2016

Защита информации

РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Общие требования

Издание официальное

Спасибо!

Александр Лискин

Руководитель лаборатории антивирусных исследований,
АО «Лаборатория Касперского»

kaspersky