

УДК 004.438С/С++:004.056

ББК 32.973.26-018

К48

**Клейн, Тобиас.**

К48 Дневник охотника за ошибками. Путешествие через джунгли проблем безопасности программного обеспечения / Т. Клейн ; пер. с англ. А. Н. Киселёва. — 2-е изд., эл. — 1 файл pdf : 241 с. — Москва : ДМК Пресс, 2023. — Систем. требования: Adobe Reader XI либо Adobe Digital Editions 4.5 ; экран 10". — Текст : электронный.

ISBN 978-5-89818-599-2

Книга «Дневник охотника за ошибками», написанная экспертом по безопасности программного обеспечения Тобиасом Клейном (Tobias Klein), рассказывает, как обнаруживаются и используются ошибки, найденные им в некоторых наиболее популярных во всем мире программных продуктах, таких как операционная система Apple iOS, медиапроигрыватель VLC, веб-браузеры и даже ядро операционной системы Mac OS X. В этом уникальном отчете вы увидите, как разработчики, по чьей вине произошли эти ошибки, исправили их — или же оказались не в состоянии это сделать.

Попутно вы познакомитесь:

- с приемами поиска ошибок, такими как идентификация и отслеживание движения пользовательских данных и инженерный анализ;
- с эксплуатацией уязвимостей, таких как разыменование нулевого указателя, переполнение буфера и преобразования типов;
- с принципами разработки концептуального программного кода, доказывающего наличие уязвимости;
- с правилами передачи извещений об ошибках производителям программного обеспечения или независимым брокерам.

Книга «Дневник охотника за ошибками» снабжена реальными примерами уязвимого кода и программ, использовавшихся для поиска и проверки ошибок. Неважно, охотитесь ли вы за ошибками только ради забавы, зарабатываете ли вы на этом или просто стремитесь сделать мир безопаснее, вы приобретете новые ценные навыки, наблюдая за тем, как действует профессиональный охотник за ошибками.

УДК 004.438С/С++:004.056

ББК 32.973.26-018

**Электронное издание на основе печатного издания:** Дневник охотника за ошибками. Путешествие через джунгли проблем безопасности программного обеспечения / Т. Клейн ; пер. с англ. А. Н. Киселёва. — Москва : ДМК Пресс, 2015. — 241 с. — ISBN 978-5-97060-294-2. — Текст : непосредственный.

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельцев авторских прав.

Материал, изложенный в данной книге, многократно проверен. Но поскольку вероятность технических ошибок все равно существует, издательство не может гарантировать абсолютную точность и правильность приводимых сведений. В связи с этим издательство не несет ответственности за возможные ошибки, связанные с использованием книги.

В соответствии со ст. 1299 и 1301 ГК РФ при устранении ограничений, установленных техническими средствами защиты авторских прав, правообладатель вправе требовать от нарушителя возмещения убытков или выплаты компенсации.

ISBN 978-5-89818-599-2

© by Tobias Klein, No Starch Press, Inc.

© Оформление, перевод на русский язык,  
ДМК Пресс, 2015



<b>Благодарности.....</b>	<b>11</b>
---------------------------	-----------

<b>Введение .....</b>	<b>12</b>
-----------------------	-----------

## **Глава 1**

<b>Выявление уязвимостей .....</b>	<b>14</b>
------------------------------------	-----------

1.1. Ради забавы и выгоды .....	15
---------------------------------	----

1.2. Универсальные приемы .....	15
---------------------------------	----

Мои личные предпочтения .....	15
-------------------------------	----

Поиск потенциально уязвимого кода .....	16
---	----

Фаззинг.....	16
--------------	----

Дополнительная литература .....	17
---------------------------------	----

1.3. Ошибки обращения с памятью .....	18
---------------------------------------	----

1.4. Используемые инструменты.....	19
------------------------------------	----

Отладчики .....	19
-----------------	----

Дизассемблеры.....	19
--------------------	----

1.5. EIP = 41414141 .....	20
---------------------------	----

1.6. Заключительное примечание .....	21
--------------------------------------	----

Примечания .....	21
------------------	----

## **Глава 2**

<b>Назад в 90-е.....</b>	<b>23</b>
--------------------------	-----------

2.1. Обнаружение уязвимости.....	24
----------------------------------	----

Шаг 1: создание списка демультимплексоров.....	24
--	----

Шаг 2: идентификация входных данных.....	25
--	----

Шаг 3: определение порядка движения входных данных.....	25
---	----

## 6 СОДЕРЖАНИЕ

<b>2.2. Эксплуатация уязвимости .....</b>	<b>27</b>
Шаг 1: Поиск образца файла в формате TiVo.....	28
Шаг 2: Определение пути достижения уязвимого кода .....	28
Шаг 3: Изменение файла в формате TiVo так, чтобы он вызывал ошибку в проигрывателе VLC.....	31
Шаг 4: Изменение файла в формате TiVo для захвата контроля над EIP .....	32
<b>2.3. Ликвидация уязвимости .....</b>	<b>34</b>
<b>2.4. Полученные уроки.....</b>	<b>39</b>
<b>2.5. Дополнение.....</b>	<b>39</b>
Примечания .....	41
<b>3.1. Обнаружение уязвимости.....</b>	<b>43</b>
<b>Глава 3</b>	
<b>Выход из зоны WWW .....</b>	<b>43</b>
Шаг 1: составление списка IOCTL-запросов, поддерживаемых ядром .....	44
Шаг 2: идентификация входных данных.....	45
Шаг 3: определение порядка движения входных данных.....	47
<b>3.2. Эксплуатация уязвимости .....</b>	<b>55</b>
Шаг 1: Вызов ситуации разыменования нулевого указателя для отказа в обслуживании .....	55
Шаг 2: использование нулевой страницы для получения контроля над EIP/RIP .....	60
<b>3.3 Ликвидация уязвимости .....</b>	<b>71</b>
<b>3.4. Полученные уроки.....</b>	<b>72</b>
<b>3.5. Дополнение.....</b>	<b>72</b>
Примечания .....	73
<b>Глава 4</b>	
<b>И снова нулевой указатель .....</b>	<b>75</b>
<b>4.1. Обнаружение уязвимости.....</b>	<b>76</b>
Шаг 1: составление списка демультимплексоров в библиотеке FFmpeg .....	76

Шаг 2: идентификация входных данных.....	76
Шаг 3: определение порядка движения входных данных.....	77
<b>4.2. Эксплуатация уязвимости .....</b>	<b>81</b>
Шаг 1: поиск образца файла в формате 4X с допустимым блоком strk .....	81
Шаг 2: изучение организации блока strk.....	81
Шаг 3: изменение содержимого блока strk для вызова ошибки в FFmpeg.....	83
Шаг 4: изменение содержимого блока strk для получения контроля над EIP .....	87
<b>4.3. Ликвидация уязвимости .....</b>	<b>92</b>
<b>4.4. Полученные уроки.....</b>	<b>96</b>
<b>4.5. Дополнение.....</b>	<b>97</b>
Примечания .....	97
<b>Глава 5</b>	
<b>Зашел и попался .....</b>	<b>99</b>
<b>5.1. Обнаружение уязвимости.....</b>	<b>99</b>
Шаг 1: составление списка зарегистрированных объектов WebEx и экспортируемых методов .....	100
Шаг 2: тестирование экспортируемых методов в браузере ...	102
Шаг 3: поиск методов объекта в двоичном файле .....	104
Шаг 4: поиск входных значений, подконтрольных пользователю .....	107
Шаг 5: исследование методов объектов.....	108
<b>5.2. Эксплуатация уязвимости .....</b>	<b>112</b>
<b>5.3. Ликвидация уязвимости .....</b>	<b>114</b>
<b>5.4. Полученные уроки.....</b>	<b>114</b>
<b>5.5. Дополнение.....</b>	<b>115</b>
Примечания .....	115
<b>Глава 6</b>	
<b>Одно ядро покорит их .....</b>	<b>99</b>
<b>6.1 Обнаружение уязвимости.....</b>	<b>117</b>

## 8 СОДЕРЖАНИЕ

Шаг 1: подготовка гостевой системы в виртуальной машине VMware для отладки ядра.....	118
Шаг 2: составление списка драйверов и объектов устройств, созданных антивирусом avast!.....	118
Шаг 3: проверка настроек безопасности устройства .....	120
Шаг 4: составление списка поддерживаемых IOCTL-запросов.....	121
Шаг 5: поиск входных данных, подконтрольных пользователю .....	128
Шаг 6: исследование обработки IOCTL-запросов .....	131
<b>6.2. Эксплуатация уязвимости .....</b>	<b>136</b>
<b>6.3. Ликвидация уязвимости .....</b>	<b>144</b>
<b>6.4. Полученные уроки.....</b>	<b>144</b>
<b>6.5. Дополнение.....</b>	<b>144</b>
Примечания .....	145

## Глава 7

<b>Ошибка, древнее чем 4.4BSD .....</b>	<b>147</b>
<b>7.1. Обнаружение уязвимости.....</b>	<b>147</b>
Шаг 1: составление списка IOCTL-запросов, поддерживаемых ядром .....	148
Шаг 2: идентификация входных данных.....	148
Шаг 3: определение порядка движения входных данных.....	150
<b>7.2. Эксплуатация уязвимости .....</b>	<b>154</b>
Шаг 1: вызов ошибки для обрушения системы (отказ в обслуживании).....	154
Шаг 2: подготовка окружения для отладки ядра.....	156
Шаг 3: подключение отладчика к целевой системе .....	156
Шаг 4: получение контроля над EIP .....	158
<b>7.3. Ликвидация уязвимости .....</b>	<b>165</b>
<b>7.4. Полученные уроки.....</b>	<b>166</b>
<b>7.5. Дополнение.....</b>	<b>166</b>
Примечания .....	167

## Глава 8

<b>Подделка рингтона .....</b>	<b>169</b>
<b>8.1. Обнаружение уязвимости.....</b>	<b>169</b>
Шаг 1: исследование аудиовозможностей смартфона	
iPhone .....	170
Шаг 2: создание фаззера и испытание телефона.....	170
<b>8.2. Анализ аварий и эксплуатация уязвимости.....</b>	<b>177</b>
<b>8.3. Ликвидация уязвимости .....</b>	<b>185</b>
<b>8.4. Полученные уроки.....</b>	<b>185</b>
<b>8.5. Дополнение.....</b>	<b>186</b>
Примечания .....	186

## Приложение А

<b>Подсказки для охотника .....</b>	<b>187</b>
<b>A.1. Переполнение буфера на стеке.....</b>	<b>187</b>
Пример: переполнение буфера на стеке в Linux .....	189
Пример: переполнение буфера на стеке в Windows .....	190
<b>A.2. Разыменование нулевого указателя.....</b>	<b>192</b>
<b>A.3. Преобразование типов в языке С .....</b>	<b>193</b>
<b>A.4. Затирание глобальной таблицы смещений .....</b>	<b>197</b>
Примечания .....	202

## Приложение В

<b>Отладка .....</b>	<b>203</b>
<b>B.1. Отладчик Solaris Modular Debugger (mdb) .....</b>	<b>203</b>
<b>B.2. Отладчик Windows (WinDbg) .....</b>	<b>205</b>
<b>B.3. Отладка ядра Windows .....</b>	<b>206</b>
Шаг 1: настройка гостевой системы в виртуальной машине	
VMware для удаленной отладки ядра .....	207
Шаг 2: изменение файла boot.ini гостевой системы.....	209
Шаг 3: настройка WinDbg в хост-машине VMware	
для отладки ядра Windows .....	209

## 10 СОДЕРЖАНИЕ

<b>В.4. Отладчик GNU Debugger (gdb) .....</b>	<b>210</b>
<b>В.5. Использование ОС Linux для отладки ядра Mac OS X .....</b>	<b>212</b>
Шаг 1: установка древней версии операционной системы Red Hat Linux 7.3 .....	212
Шаг 2: получение всех необходимых пакетов программного обеспечения .....	213
Шаг 3: сборка отладчика Apple в системе Linux .....	213
Шаг 4: подготовка окружения отладки .....	216
Примечания .....	216
 <b>Приложение С</b>	
<b>Методы защиты .....</b>	<b>218</b>
<b>С.1. Приемы защиты от эксплуатации уязвимостей .....</b>	<b>218</b>
Случайная организация адресного пространства (ASLR) .....	219
Защита от срыва стека: Security Cookies (/GS) .....	219
Stack-Smashing Protection (SSP) и Stack Canaries .....	219
Защита от выполнения данных NX и DEP .....	219
Выявление механизмов защиты от эксплойтов .....	220
<b>С.2. RELRO .....</b>	<b>223</b>
Испытание 1: поддержка частичного режима RELRO .....	224
Испытание 2: поддержка полного режима RELRO .....	225
В заключение .....	226
<b>С.3. Solaris Zones .....</b>	<b>227</b>
Терминология .....	227
Настройка неглобальной зоны в Solaris .....	228
Примечания .....	230
 <b>Предметный указатель .....</b>	<b>233</b>
<b>Об авторе .....</b>	<b>239</b>