

УДК 004.438С/С++:004.056

ББК 32.973.26-018

К48

К48 Тобиас Клейн

Дневник охотника за ошибками. Путешествие через джунгли проблем безопасности программного обеспечения. Пер. с англ. Киселев А. Н. – М.: ДМК Пресс. – 240 с.: ил.

ISBN 978-5-97060-294-2

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. Независимо, 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.

Original English language edition published by No Starch Press, Inc., 38 Ringold Street, San Francisco, CA 94103, USA. Copyright (c) 2011 by No Starch Press, Inc.. Russian-language edition copyright (c) by ДМК Пресс. All rights reserved.

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.

ISBN 978-1-59327-385-9 (англ.)

ISBN 978-5-97060-294-2 (рус.)

© by Tobias Klein, No Starch Press, Inc.

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



Благодарности.....	11
---------------------------	-----------

Введение	12
-----------------------	-----------

Глава 1

Выявление уязвимостей	14
------------------------------------	-----------

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

Назад в 90-е.....	23
--------------------------	-----------

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

Шаг 1: создание списка демультимплексов	24
---	----

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

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

6 СОДЕРЖАНИЕ

2.2. Эксплуатация уязвимости	27
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
2.3. Ликвидация уязвимости	34
2.4. Полученные уроки.....	39
2.5. Дополнение.....	39
Примечания	41
3.1. Обнаружение уязвимости.....	43
Глава 3	
Выход из зоны WWW	43
Шаг 1: составление списка IOCTL-запросов, поддерживаемых ядром	44
Шаг 2: идентификация входных данных.....	45
Шаг 3: определение порядка движения входных данных.....	47
3.2. Эксплуатация уязвимости	55
Шаг 1: Вызов ситуации разыменования нулевого указателя для отказа в обслуживании	55
Шаг 2: использование нулевой страницы для получения контроля над EIP/RIP	60
3.3 Ликвидация уязвимости	71
3.4. Полученные уроки.....	72
3.5. Дополнение.....	72
Примечания	73
Глава 4	
И снова нулевой указатель	75
4.1. Обнаружение уязвимости.....	76
Шаг 1: составление списка демультимплексоров в библиотеке FFmpeg	76

Шаг 2: идентификация входных данных.....	76
Шаг 3: определение порядка движения входных данных.....	77
4.2. Эксплуатация уязвимости	81
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
4.3. Ликвидация уязвимости	92
4.4. Полученные уроки.....	96
4.5. Дополнение.....	97
Примечания	97
Глава 5	
Зашел и попался	99
5.1. Обнаружение уязвимости.....	99
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
5.2. Эксплуатация уязвимости	112
5.3. Ликвидация уязвимости	114
5.4. Полученные уроки.....	114
5.5. Дополнение.....	115
Примечания	115
Глава 6	
Одно ядро покорит их	99
6.1 Обнаружение уязвимости.....	117

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
6.2. Эксплуатация уязвимости	136
6.3. Ликвидация уязвимости	144
6.4. Полученные уроки.....	144
6.5. Дополнение.....	144
Примечания	145

Глава 7

Ошибка, древнее чем 4.4BSD	147
7.1. Обнаружение уязвимости.....	147
Шаг 1: составление списка IOCTL-запросов, поддерживаемых ядром	148
Шаг 2: идентификация входных данных.....	148
Шаг 3: определение порядка движения входных данных.....	150
7.2. Эксплуатация уязвимости	154
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
7.3. Ликвидация уязвимости	165
7.4. Полученные уроки.....	166
7.5. Дополнение.....	166
Примечания	167

Глава 8

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

Приложение А

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

Приложение В

Отладка	203
B.1. Отладчик Solaris Modular Debugger (mdb)	203
B.2. Отладчик Windows (WinDbg)	205
B.3. Отладка ядра Windows	206
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

В.4. Отладчик GNU Debugger (gdb)	210
В.5. Использование ОС Linux для отладки ядра Mac OS X	212
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
 Приложение С	
Методы защиты	218
С.1. Приемы защиты от эксплуатации уязвимостей	218
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
С.2. RELRO	223
Испытание 1: поддержка частичного режима RELRO	224
Испытание 2: поддержка полного режима RELRO	225
В заключение	226
С.3. Solaris Zones	227
Терминология	227
Настройка неглобальной зоны в Solaris	228
Примечания	230
 Предметный указатель	233
Об авторе	239