RutheniumOS. Забота о себе, или зачем нужна ещё одна приватная ОС на базе AOSP

24.02.2024

Введение

> Меня зовут Александр, занимаюсь обеспечением приватности и мобильной безопасностью. Вместе с командой разрабатываем RutheniumOS - приватную и безопасную ОС.

Ruthenium OS

План:

- Любовь и корпорации, или откуда взялись неофициальные прошивки.
- Открытость != приватность: какие сервисы AOSP передают информацию в Google.

- А давайте соберём AOSP: вода под камнями, опыт портирования.
- Сапожник ходит без рута: как после вольностей в настройках вернуть себе прежнюю безопасность ОС Android.

Сегодня мы поговорим про ОС Android или ОС на базе AOSP, о самых знаковых для становления индустрии смартфонах, о том, что такое прошивки, какими они бывают, почему они появились и чем они нас не устроили, что и стало причиной появления RutheniumOS, расскажу о том, чем занимаемся, и что нас отличает от остальных, потом отвечу на возникшие вопросы, но сначала давайте условимся, какую терминологию будем использовать.

Глоссарий

AOSP - Android Open Source Project. Общедоступная кодовая база, на которой построено бесчисленное множество ОС. Да, всё созданное на базе AOSP сами Google признают полноценной ОС[^1]

Android - это ОС, разработанная компанией Google для использования на мобильных устройствах, таких как смартфоны и планшеты. ОС Android создается благодаря сотрудничеству между и производителями оборудования и самой Google. Ключевым отличием от **AOSP** является наличие **Google Management Services (GMS)** - экосистемы, отвечающей за работу с ПО. Установка из Google Play, платежи, сервисы позиционирования и прочее.

Google Services/Gaps - реализация GMS для пользовательских прошивок.

XDA (2006) - крупнейший форум, посвященный Android разработке, в том числе и неофициальных прошивок

4PDA (2005) - примерный российский аналог XDA

Custom ROM (на 4PDA называется неофициальная прошивка) - термин "прошивка" происходит из той поры, когда телефон на самом деле нужно было прошивать, правильнее говорить ОС на базе Android, (о чем говорится в официальной документации) но мы будем использовать устоявшееся название.

root (рут) - в контексте доклада, права суперпользователя.

блоб - бинарный обьект. Тут под блобами чаще имеются ввиду драйверы устройств

Безопасность - процесс нацеленный на своевременное выявление и устранение уязвимостей в исходном коде.

Приватность - процесс, нацеленный на сохранность персональных данных и минимизацию их утечки.

- Любовь и корпорации, или откуда взялись неофициальные прошивки.

1 история Android inc и OS Android до покупки компанией Google

ОС Android была создана компанией Android Inc., в 2003 году, как операционная система для цифровых фотокамер. Изначально создатели компании Android inc увидели, что софт для тогдашних

камер оставляет желать много лучшего. Так что с определенными допущениями можно сказать, что мы имеем дело с ОС для цифровых камер, забавно, да? Вектор на смартфоны был взят только в 2004. В 2005 Android Inc., была куплена компанией Google. Потом выходцы из этой компании нас еще не раз порадуют, а пока их покупает Google и ОС начинает активно развиваться. В октябре 2008, 16 лет назад, состоялся релиз первого Android-смартфона **HTC Dream: G1** Показать вам его я не могу, но у меня есть кое-что получше. Нет, не рисунок телефона, а DevKit - инженерный прототип, который рассылался разработчикам. Первый, и насколько мне известно, единственный телефон, который с завода шел с рутом. Корпорация добра использовала в нем аккумулятор от Nokia и проприетарный USB-разъем. Ну что же - вот и он.

2 откуда взялись неофициальные прошивки

Поскольку iPhone был представлен январе 2007, Google были в невыгодном положении и вынуждены были спешить с релизом. Что мы имели на старте в Android? Очень сырой продукт, фрагментированный (разные устройства, разные лаунчеры, разный функционал) рынок но

открытость его подкупала энтузиастов. В ноябре 2008 года на xda появляется пользователь под ником JesusFreke, который создает одну из первых прошивок.

3 о судьбе, развитии, смерти и перерождении самой известной прошивки

После ухода JesusFreke на покой Стефани Кондик (Cyanogen) продолжила работу, так и появился легендарный **CyanogenMOD**.

(Cyanogate) Отделение Google Apps

В 2009 году Google присылает письмо с требованием прекратить использование CyanogenMod из-за распространения приложений Google, в частности Android Market. Проблема была в том, что CyanogenMod распространил более новую версию Android Market, версию 1.6, до того, как Google опубликовал её. В 2012 году CyanogenMod был на грани закрытия из-за юридических проблем с Google. После удаления Google Apps (GApps) из состава прошивки Google оставил CyanogenMod в покое[^2].

Стефани работала над CyanogenMod в свободное время, пока не получила предложение от Карла Пэя и Курта Макмастера о создании телефона с CyanogenMod в качестве операционной системы.

Прошивка от компании OnePlus была основана на CyanogenMod и стала успешной благодаря своей ориентации на сообщество и хорошим характеристикам устройств. OnePlus One был первым телефоном компании с операционной системой CyanogenMod и стал популярным среди

энтузиастов. Однако через некоторое время Стефани продала эксклюзивные права на Cyanogen OS индийской компании Micromax, что вызвало проблемы с продажей OnePlus One в Индии, которая являлась важным рынком сбыта для OnePlus. OnePlus пришлось создать новую ОС - Oxygen OS, из-за невозможности использовать Cyanogen OS.

Компания Cyanogen пыталась создать свою операционную систему, но не смогла заработать деньги. В июле 2016 года уволили 100 сотрудников и закрыли офис в Сиэтле. В декабре 2016 года опубликовали сообщение о создании Lineage OS, которая стала продолжением CyanogenMod. Good night, sweet prince! (!перечеркнуть лого!)

Затем, как наследник, свет увидела наиболее распространенная в наши дни прошивка LinageOS, но это уже совсем другая история, которая выходит за рамки этого доклада.

- Открытость != приватность: какие сервисы AOSP передают информацию в Google

Если помнить, что Google в первую очередь рекламная компания и получает доход от рекламы, факт того, что Android собирает в 20 раз больше[^3] телеметрии, чем iOS становится не только неудивительным но и ожидаемым. Телефоны на Android и iOS делятся данными о своих основных характеристиках со своими производителями в среднем каждые 4,5 минуты. Передаются IMEI, серийный номер оборудования, серийный номер SIM-карты, номер телефона, IMSI, WiFi MAC.

Давайте разберем каналы и причины утечек информации.

Важно понимать, что сама по себе доступность исходных кодов ничего не гарантирует, кроме возможности что-то с ними сделать. Ни безопаснее, ни приватнее от этого продукт не становится. Да, AOSP со свежими патчами достаточно безопасна, но что с данными пользователя, как насчет пресловутой приватности? Даже собранный из исходников AOSP использует серверы корпорации добра

DNS - в качестве серверов по умолчанию используются принадлежащие компании Google IPv4: 8.8.8.8, 8.8.4.4, IPv6: 2001:4860:4860::8888, 2001:4860:4860::8844

Captive Portal Check - clients3.google.com

connectivity check - connectivitycheck.gstatic.com

aGPS - IMSI supl.google.com

AOSP Webview - WEBRTC/JS

NTP - time.android.com

Чем же эти пункты нам грозят?

DNS - позволяет отслеживать, какие сайты посещает пользователь.

Captive portal Check и connectivity check - проверяет подключение и наличие порталов захвата в сети подключаясь к серверам Google

aGPS - передает на серверы Google информацию о местонахождении, обогащая её данными от провайдера, а так же передавая IMSI, что позволяет связать эту информацию с конкретным номером, и как следствие, конкретным человеком

Webview - встроенный движок, который предоставляет возможность отображения вэб-страниц приложениям, у которых такая возможность не реализована самостоятельно - уязвим для атак злоумышленников, которые используют его для рендеринга поддельных страниц клиент-банка и прочих сайтов.

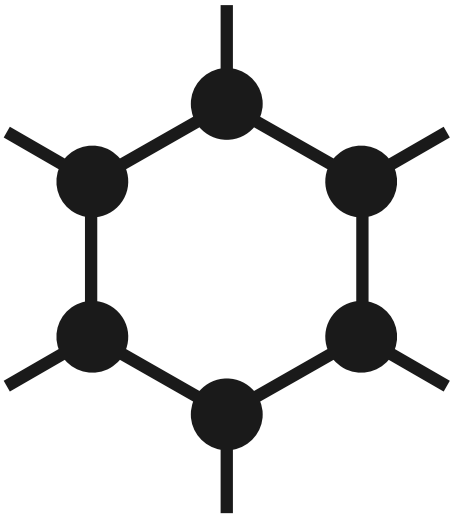
Использование NTP от Google позволяет, в теории, отследить местоположение устройства.

> К слову, практически во всех пользовательских прошивках, за исключением ориентированных на безопасность, эти проблемы присутствуют, даже больше скажу - правки закрывающие их не принимаются разработчиками.

Казалось бы, частично нам может помочь root, но он делает систему ещё более уязвимой, поскольку требует разблокировки загрузчика, что в свою очередь позволяет в дальнейшем установить на устройство произвольное ПО, которое переживет сброс до заводских настроек.

4 про ОС, ориентированные на безопасность, их обзор и сравнение.

Чем отличаются безопасность от приватности. Ложное чувство защищенности и немного конспирологии.



GrapheneOS, основанная Даниэлем Микеем в конце 2014 года, изначально была личным проектом, сосредоточенным на улучшении конфиденциальности и безопасности. Сперва он создал порт malloc из OpenBSD в libc Bionic из Android и порт патчей ядра PaX в ядра поддерживаемых устройств. Проект быстро расширился и включил в себя работу по низкоуровневому усилению инструментария компилятора и Bionic. В конце 2015 года в качестве основного спонсора GrapheneOS, ранее известной как CopperheadOS, была зарегистрирована компания. Предполагалось, что компания будет обслуживать потребности проекта с открытым исходным кодом, но она не выполнила своих обещаний и больше не была связана с проектом. В 2018 году компания была захвачена генеральным директором, который попытался захватить и проект, однако безрезультатно. Удалось лишь взять под контроль инфраструктуру и присвоить пожертвования, но проект успешно развивался и без этого. С тех пор компания мошеннически заявляла о своем праве собственности и авторстве на проект, занимаясь дезинформацией и преследованием участников. После отделения от бывшего спонсора проект был ребрендирован в AndroidHardening и GrapheneOS, продолжая оставаться независимым проектом с открытым исходным кодом. GrapheneOS Foundation был создан как некоммерческая организация в Канаде в марте 2023 года, чтобы заниматься приемом и распределением пожертвований.

Теперь давайте взглянем на аналогичные решения.

1. CalyxOS

CalyxOS - операционная система, цель которой - дать пользователям возможность управлять своей цифровой жизнью. Она построена на таких принципах, как Privacy By Design, которые ставят интересы пользователей во главу угла на каждом этапе проектирования и разработки. CalyxOS включает в себя хорошие настройки по умолчанию, дизайн, ориентированный на

конфиденциальность, дизайн, ориентированный на пользователя, и сквозную безопасность. Система не хранит данные в "облаке" Google и не сообщает о своем местонахождении Google, а также включает в себя приложения, ориентированные на безопасность, такие как Signal и Tor Browser. CalyxOS также включает в себя встроенные бесплатные VPN-сервисы, регулярные обновления безопасности и seedVault для безопасного резервного копирования. Платформа разработана для удовлетворения потребностей правозащитников, журналистов, юристов, политических и общественных активистов в конфиденциальности и безопасности, но в то же время является удобной и полезной для всех. CalyxOS только начинает свою работу, но для реализации ее цели - обеспечения безопасности и конфиденциальности для всех - необходимо приложить еще больше усилий.

2. DivestOS:

DivestOS - это проект, которым Тави увлекается с 2014 года и целью которого является продление срока службы устройств, повышение конфиденциальности пользователей и безопасности. Несмотря

на то, что DivestOS не является полностью открытой, она решает такие проблемы безопасности, как проприетарные блобы, устранение недостатков прошивки, загрузчиков и древние ядра.

5 о судьбе и вкладе в это одного человека, ключевого для индустрии

Q: Видение целевой аудитории ориентированных на приватность ос. A: Несмотря на свою чёткую ориентированность на приватность и безопасность, мы стараемся делать так чтобы GrapheneOS мог использовать каждый/каждая

Q: Видение будущего мобильных ОС A: В ближайшие пару лет мы надеемся увидеть больше смартфонов с поддержкой MTE.

Также надеемся что MTE будут использовать на стоке, так как сейчас он по дефолту выключен на 8 поколении пикселей (единственные смартфоны с поддержкой MTE сегодня)

- А давайте соберём AOSP: вода под камнями, опыт портирования.

6 про причины появления и историю RutheniumOS

За каждым начинанием стоит идея. А за идеей необходимость. Однажды я задумался, сколько и какой информации получают из самого близкого нам устройства - смартфона. Никаких теорий заговоров, просто бизнес. Обогащение данных, более точное таргетирование рекламы и прочее. (Я не рассматриваю случай, когда человек интересен спецслужбам. Тут уже ничего не поможет) Из доступного на рынке, если не углубляться в дебри альтернативных операционных системы, можно выделить несколько решений. Все они хороши по своему, но не лишены недостатков. Критических, на мой взгляд. Допустим что толку от ОС, которая позиционирует себя как нацеленная на приватность и безопасность, если обновления выходят с большой задержкой, или что толку от безопасной, обновляемой системы, если у нее не настроен правильно браузер и дизайн выдает в ней неоригинальную. Это если совсем по верху взять. . В силу этих причин было решено взять лучшее от всех миров. Сбалансированную с точки зрения безопасности ос, которая не выдает себя но способна предоставить полезный функционал. Сейчас мы заняты именно этим, программированием функций, анализом работы Android на низком уровне и прочее.

7 про процесс работы, планы по внедрению функций и какой используем инструментарий

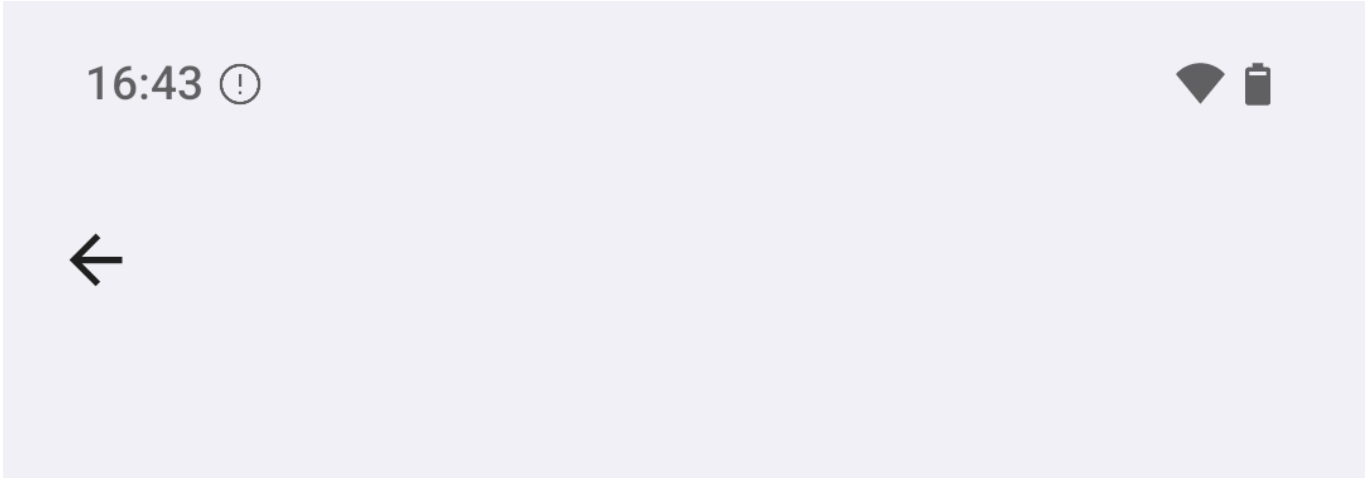
Основная угроза в мире безопасности это человеческий фактор, а потому в плане ликвидации и предотвращения ошибок в работе ПО доверять нельзя никому, особенно производителю, которых много раз ловили на подделке информации об обновлениях безопасности ОС.

Для нас самым важным источником информации об уязвимостях является Android Security Bulletin (далее ASB), это ежемесячно выходящая статья с разбором уязвимостей компонентов OS и ссылками на патчи, закрывающие эти уязвимости.

Что такое Бюллетень безопасности?

Каждая уязвимость в списке имеет номер Common Vulnerabilities and Exposures (CVE), а также соответствующие ссылки, тип уязвимости, оценку серьезности и версию AOSP. Несмотря на кажущуюся простоту, на самом деле всё не так прозрачно. Многие из этих производителей также публикуют собственные бюллетени безопасности.

Соответствие исправлений, примененных к операционной системе на конкретном устройстве определенному бюллетеню называется уровнем безопасности Android.



Версия Android

Версия Android
14

Обновление системы безопасности Android
5 января 2024 г.

Прошивка модуля связи
g5123b-125137-231014-B-10950115

Bootloader version
bluejay-1.3-10825045

Версия ядра
5.10.208-android13-4-g9fafa9e05ab6
#1 Mon Jan 22 08:54:27 UTC 2024

Номер сборки
UQ1A.240105.002.2024020800

Давайте теперь рассмотрим конкретный пример такого бюллетеня за январь 2024. Наиболее серьезной из этих проблем является высокая уязвимость в компоненте Framework, которая может привести к локальному повышению привилегий без дополнительных привилегий на выполнение. Оценка серьезности основывается на эффекте, который эксплуатация уязвимости может оказать на затронутое устройство, при условии, что платформа и службы защиты отключены в целях разработки или успешно обойдены. Для примера возьмём уязвимость **CVE-2024-0023**

Framework

The most severe vulnerability in this section could lead to local escalation of privilege with no additional execution privileges needed.

CVE	References	Type	Severity	Updated AOSP versions
CVE-2023-21245	A-222446076 [2]	EoP	High	11, 12, 12L, 13, 14
CVE-2024-0015	A-300090204	EoP	High	11, 12, 12L, 13
CVE-2024-0018	A-300476626	EoP	High	11, 12, 12L, 13, 14
CVE-2024-0023	A-283099444 [2]	EoP	High	11, 12, 12L, 13, 14
CVE-2024-0019	A-294104969	ID	High	12, 12L, 13, 14

Уязвимости присвоен номер CVE-2024-0023, она затрагивает framework/av, ссылка на патч в репозитории AOSP A-283099444, тип уязвимости Повышение привилегий, приоритет – высокий, уязвимы версии Android с 11 по 14. Перейдя по ссылке, чтобы посмотреть описание патча мы увидим невразумительное:

```
Codec2BufferUtils: Use cropped dimensions in RGB to YUV conversion
```

Чтобы облегчить работу наша команда разработки написала утилиту **harvester** Она отвечает за анализ ASB.
Вот пример запуска:

```
harvester.py --help
usage: harvester.py [-h] [-url {last,all}] [-unpublish] [-text] [-output
OUTPUT] [-android ANDROID] [-data DATA] [-translate_text TRANSLATE_TEXT]

Android Security Bulletin Harvester

options:
  -h, --help            show this help message and exit
  -url {last,all}       Parse needed Security Bulletin or last or all from
https://source.android.com/docs/security/bulletin/
  -unpublish            Show unpublished CVE
  -text                 Output in text format
  -output OUTPUT        File name for output text
  -android ANDROID      Filter CVEs by Android version
  -data DATA            Filter data cve
  -translate_text TRANSLATE_TEXT
                        Translate ru out data
```

Запуск со следующими параметрами позволяет получить информацию из последнего бюллетеня безопасности в текстовом виде, скачать и разложить по папкам патчи, информация будет касаться 14 версии AOSP, так же программа возьмет из базы уязвимостей описание и переведет его на русский, результат же запишет в файл 2024.md

```
harvester.py -url last -text -output 2024.md -data 2024 -android 14 -
translate_text ru
```

Информация по нашей уязвимости CVE-2024-0023 будет выглядеть вот так

CVE-2024-0023

Тип уязвимости: Высокая, EoP.

Уязвимые версии: 11, 12, 12L, 13, 14

Ссылка на патч(и):
https://android.googlesource.com/platform/frameworks/av/+/30b1b34cfd5abfcfee759e7d13167d368ac6c268

Краткое описание уязвимости:

В ConvertRGBToPlanarYUV Codec2BufferUtils.cpp возможна запись за пределами границ из-за неправильной проверки границ. Это может привести к локальному повышению привилегий без необходимости дополнительных привилегий выполнения. Для эксплуатации не требуется взаимодействие с пользователем.

Мы считаем, что так гораздо нагляднее. В будущем планируется добавить следующий функционал: Проверка репозиториев на предмет применения патчей, если не применен - сообщать об этом оператору, чтобы он мог взять ошибку в работу. Как следующий этап - проверка двоичных файлов на

предмет того, применялись к ним патчи или нет. Планируется так же написание утилиты, которая поможет сократить количество ошибок, за счет вычисления необязательных компонентов системы. Также планируется внедрить файерволл на уровне сети, в дополнение к имеющемуся и работающему на уровне разрешений.

- Сапожник ходит без рута: как после вольностей в настройках вернуть себе прежнюю безопасность ОС Android.

Мне не известны способы устранения каналов утечки в системе, которая поставляется с устройством, без использования root, что сводит на нет все усилия по обеспечению безопасности. Потому единственный путь, который я вижу - редактирование исходных кодов, сборка системы и последующая установка на устройство с блокировкой загрузчика.

Примечания и использованные материалы

[^1]: Android is an operating system for a wide array of devices with different form factors. The documentation and source code for Android is available to anyone as the Android Open Source Project (AOSP). You can use AOSP to create custom variants of the Android OS for your own devices.

[^2]: Такое разделение существует до сих пор, оно позволяет пользователям выбирать и устанавливать GApps в соответствии со своими предпочтениями. Кроме того, это позволяет разработчикам пользовательских прошивок соблюдать требования лицензирования, предоставляя пользователям гибкость в принятии решения о том, хотят ли они использовать фирменные приложения и сервисы Google.

[^3]: Mobile Handset Privacy: Measuring The Data iOS and Android Send to Apple And Google

---

Google announces open-source mobile phone OS, Android

Презентация Android

Britanica Android OS history

History of LineageOS

Mobile Monday - Rich Miner: History of Android

Эволюция Nexus

Эволюция Pixel

Подкаст о CyanogenMOD

CyanogenMOD shuting down (31.12.2016)

Что означает смерть CyanogenMod

История GrapheneOS

История CalyxOS

История DivestOS

История 4PDA

When Phones Were Fun: The Sidekick (2002-2010)

HTC Dream: G1 раздел на XDA

Android, iOS beam telemetry to Google, Apple even when you tell them not to

Android sends 20x more data to Google than iOS to Apple

Как root-права и альтернативные прошивки делают ваш android смартфон уязвимым

Locking/Unlocking the Bootloader

Android. OS privacy guard

Компания Google перевела в разряд устаревших приложения Dialer и Messaging, поставляемые в репозитории AOSP. Объявлено, что в будущем данные приложения, предоставляющие интерфейс для осуществления звонков и работы с SMS, будут удалены из репозитория AOSP, что потребует при создании сборок на основе AOSP обязательного использования внешних приложений для реализации данной функциональности.

При этом объявленные устаревшими приложения обычно не использовались на практике и рассматривались в основном как рабочие прототипы с примерами организации работы с вызовами и текстовыми сообщениями. Поставляемые производителями телефонов прошивки и создаваемые на основе AOSP независимые сборки, такие как LineageOS, использовали собственные реализации приложений Dialer и Messaging.