1 Слайд

Первое упоминание об баге в IOS

С чего же все началось? 11 февраля 2016 года исследователь **Зак Стрэйли** опубликовал на Youtube видео, в котором демонстрирует свое поразительное и до странности простое открытие: ручная установка даты iPhone или iPad на 1 января 1970 превращало устройство в обычный кирпич, который не работал. Данное состояние называется BootLoop

--КЛИК--

2 Слайд

Что такое BOOTLOOP?

Bootloop – это состояние смартфона, при котором он запускает циклическую перезагрузку системы и не может запустить ее. Термин происходит от сочетания английских слов boot (загрузка) и loop (петля). На экране устройства отображается логотип производителя (или ОС Android), но дальше дело не идет. Отключения питания, принудительная перезагрузка и другие методы в таком случае не помогают.

--КЛИК--

3–4 Слайд

Что же приводило девайсы Apple в данное состояние? + Пример

У iOS-устройств от Apple на архитектуре x64 на процессорах A7, A8, A8X, A9 и A9X существует проблема как Unix-системы: если перевести время на устройстве с 64-битным процессором под управлением iOS на час ночи первого января 1970 года и перезагрузить устройство, будучи в часовом поясе от UTC +1:30 и больше, то после перезагрузки устройства оно не будет включаться, на экране постоянно будет отображаться логотип Apple. Происходит это из-за разницы в часовых поясах, то есть: если перевести время на 1:00 1 января 1970 года в часовом поясе UTC +1:30 или больше, то счётчик Unix-времени уходит в минус, что система понять не в состоянии, так как отсчёт ведётся от UTC, вследствие чего устройство зависает.

--КЛИК--

UTC (Universal Temps Coordinated) – это всемирное координированное время. Основано на международном атомном времени (TAI). TAI – средневзвешенное значение сигналов от более чем 200 атомных часов, расположенных в 70 научных лабораториях по всему миру.

--КЛИК--

5–7 Слайд

Ты нас обманул? Сертификаты!!!

--КЛИК--

Одной из возможных причин данной проблемы является то, что большинство приложений на IOS настроены на использование сертификатов безопасности, которые шифруют данные, передаваемые их на устройство пользователя и обратно. Эти сертификаты шифрования перестают работать правильно, если системное время и дата на мобильных устройствах пользователя установлены на год, предыдущий выдаче сертификата.

--КЛИК--

Исследователи безопасности Патрик Келли и Мэтт Харриган заявили, что это, по-видимому, создает хаос для большинства приложений.

--КЛИК--

Они начинают на устройстве конкурировать за ресурсы, быстро подавляя вычислительную мощность устройства настолько, что их тест показал, что устройство всего за несколько минут достигло 54 градуса по Цельсию.

--КЛИК--

Поскольку настройки даты и часов на затронутом устройстве необъяснимо и устрашающе начали отсчет в обратную сторону.

--КЛИК--

8–13 Слайд

Тролли и злоумышленники

--КЛИК--

В промежуток времени, между тем как вышло первое упоминание и фиксом данного бага от Apple на горизонте появлялись тролли в интернете и злоумышленники.

--КЛИК--

Обычно на просторах форумов или социальных сетей можно было встретить данную картинку, в которой говорится, что установка даты 1970 года позволит тебе получить новый хиппи-дизайн, новый шрифт и несколько прикольных обоев. Некоторые пользователи велись на данную уловку и ломали себе устройства.

--КЛИК--

Но были более изощрённые идеи как сломать устройства другим пользователям. Все те же Патрик Келли и Мэтт Харриган нашли гениальную вещь. Продукты Apple, например, как Ipad и Iphone предназначены для автоматического подключения к беспроводным сетям, которые они видели раньше. То есть, если вы когда-то подключались к сети с названием например “FreeWiFi”. То в последствии ваше устройство может подключаться ко всем сетям без пароля с названием “FreeWiFi”. Это ещё одна уязвимость, которая была в продукции Apple. Злоумышленник, с такой сетью может попытаться, например проверить, изменить или перенаправить любой сетевой трафик устройств, которые невольно подключаются к его вредоносной сети.

--КЛИК--

Именно это и сделали Келли и Харриган в своих тестах. Они поняли, что устройства Apple постоянно проверяют различные серверы “Протокола сетевого времени” (NTP) по всему миру, чтобы синхронизировать свои внутренние часы даты и времени. Они создали свою тестовую сеть под название PhoneBreaker. Она заставляла загружать обновления времени и даты со своего (злого) сервера времени NTP. После чего дата изменялась на одну адскую дату 1 января 1970 года. На Iphone’ах сетевое время обновлялось через GSM, но это никак не мешало сделать то же самое и через GSM (глобальный стандарт мобильной цифровой связи).

NTP (Network Time Protocol) — сетевой протокол для синхронизации внутренних часов компьютера с использованием сетей с переменной латентностью.

«Вполне вероятно, что эту уязвимость можно использовать через GSM, используя OpenBTS или OpenBSC для установки времени», - сказал Келли.

это проекты, пытающиеся выполнить функцию GSM-сети с открытыми исходниками.

Крейтон согласился, сказав, что его собственный опыт тестирования и эксплуатации сети NinjaTel

Так же было подмечено, что при установки данной даты переставал работать практически весь веб-трафик и обычные пользователи в таких ситуациях перезагружали свои устройства, надеясь, что все исправиться.

--КЛИК--

Как вы думаете, какие 2 вещи использовались для создания данного теста?

--КЛИК--

Само из себя аппаратное обеспечение для данной атаки представляло обычный Raspberry Pi с антенной Alfa для усиления сигнала сети. Его можно было собрать, заказав детали на AliExpress всего за 50-70 долларов.

--КЛИК--

14-18 Слайд

Исправление ошибки

--КЛИК--

Пользователи интернета сами нашли решение как исправить данный баг состояния телефона.

--КЛИК--

Можно было просто вытащить из Apple устройства аккумулятор и подождать, пока устройство обесточится полностью. После всего вернуть аккумулятор обратно и включить. Тогда время само сбросится до положительного значения и начнет загружать систему.

--КЛИК--

Но некоторые пользователи могли повредить устройства т.к. крышка IOS устройств так просто не снимается, как у других производителей. Поэтому они требовали Apple исправить баг.

--КЛИК--

31 марта 2016 года вышло наконец-то обновление, которое так долго ждали. Оно исправляло данную ошибку.

--КЛИК--

Но как вы думаете как? Оно просто запрещало ставить дату ниже 2001 года.

--КЛИК--

18 Слайд

Подведение итогов

Баг был опасен для пользователей и понес им и самой компании убытки. На этом все!

Ну ладно. Не будем издеваться над владелицами Айфонов. Apple все таки пофиксили баг с сертификатами и вернули возможность ставить дату ниже 1970 года обратно. Но как именно они это починили остается секретом т.к. компания Apple не хотела ещё больше распространять плохих слухов.

19 Слайд

ББ (Спасибо за внимание)