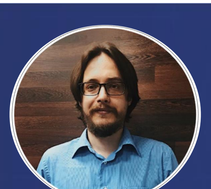
Что принесет за собой iOS 14?



Клюев Даниэль

специалист по исследованию iOS-устройств

Сегодня вышла iOS 14.0

Обновляются все устройства начиная с A9 (iPhone 6s)

iOS 14.0: что нового

— виджеты, библиотека приложений, блиц-приложения и прочие малоинтересные вещи;

— обновили протокол снятия iTunes бэкапов, сломав поддержку libimobiledevice;

— обновили протоколы для облачных сервисов, включая резервные копии;

— новые проблемы для джейлбрейков;

— много новых локально хранящихся данных.

iOS 14.0 и джейлбрейки

— три команды заявили о найденных в iOS 14 уязвимостях, позволяющих повысить привилегии;

— Pangu показали тизер рабочего джейлбрейка для iOS 14;

— попытка закрыть джейлбрейки на основе checkm8;

— команда checkra1n уже подготовила бета-версию под iOS 14, “eta s0n”;

— ряд исправлений уязвимостей, а следовательно джейлбрейк для 13.7;

— применение Memory Tagging Extension под вопросом.

ИСПРАВИТЬ НЕИСПРАВИМОЕ: iOS 14.0 и checkm8

— изменения в iBoot: изменилась схема перехода в трамплин iOS;

— новые проверки на запись данных в системный раздел;

— новые проверки на запуск приложений;

— значительные изменения в SEPOS.

ИСПРАВИТЬ НЕИСПРАВИМОЕ: iOS 14.0 и checkm8

Защиты и их отключение

```
com.apple.filesystems.apfs:__text:FFFFFFF00688D4A8 E8 02 70 37              TBNZ            W8, #0xE, loc_FFFFFFF00688D504 ; Test and Branch Non-Zero
com.apple.filesystems.apfs:__text:FFFFFFF00688D4AC 94 32 00 35              CBNZ            W20, loc_FFFFFFF00688DAFC ; Compare and Branch on Non-Zero
com.apple.filesystems.apfs:__text:FFFFFFF00688D4B0 37 05 00 37              TBNZ            W23, #0, loc_FFFFFFF00688D554 ; Test and Branch Non-Zero
com.apple.filesystems.apfs:__text:FFFFFFF00688D4B4 68 6A 40 F9              LDR             X8, [X19,#0xD0] ; Load from Memory
com.apple.filesystems.apfs:__text:FFFFFFF00688D4B8 08 1D 40 F9              LDR             X8, [X8,#0x38] ; Load from Memory
com.apple.filesystems.apfs:__text:FFFFFFF00688D4BC C8 04 28 36              TBZ             W8, #5, loc_FFFFFFF00688D554 ; Test and Branch Zero
com.apple.filesystems.apfs:__text:FFFFFFF00688D4C0 E0 03 13 AA              MOV             X0, X19 ; Rd = Op2
com.apple.filesystems.apfs:__text:FFFFFFF00688D4C4 A2 DC FD 97              BL              sub_FFFFFFF00680474C ; Branch with Link
com.apple.filesystems.apfs:__text:FFFFFFF00688D4C8 60 04 00 34              CBZ             W0, loc_FFFFFFF00688D554 ; Compare and Branch on Zero
com.apple.filesystems.apfs:__text:FFFFFFF00688D4CC F4 03 00 AA              MOV             X20, X0 ; Rd = Op2
com.apple.filesystems.apfs:__text:FFFFFFF00688D4D0 68 72 40 F9              LDR             X8, [X19,#0xE0] ; Load from Memory
com.apple.filesystems.apfs:__text:FFFFFFF00688D4D4 08 6D 40 F9              LDR             X8, [X8,#0xD8] ; Load from Memory
com.apple.filesystems.apfs:__text:FFFFFFF00688D4D8 08 81 13 91              ADD             X8, X8, #0x4E0 ; Rd = Op1 + Op2
com.apple.filesystems.apfs:__text:FFFFFFF00688D4DC 69 6A 40 F9              LDR             X9, [X19,#0xD0] ; Load from Memory
com.apple.filesystems.apfs:__text:FFFFFFF00688D4E0 29 25 40 B9              LDR             W9, [X9,#0x24] ; Load from Memory
com.apple.filesystems.apfs:__text:FFFFFFF00688D4E4 29 05 00 11              ADD             W9, W9, #1 ; Rd = Op1 + Op2
com.apple.filesystems.apfs:__text:FFFFFFF00688D4E8 6A 86 40 F9              LDR             X10, [X19,#0x108] ; Load from Memory
com.apple.filesystems.apfs:__text:FFFFFFF00688D4EC 1F A8 01 71              CMP             W0, #0x6A ; 'j' ; Set cond. codes on Op1 - Op2
com.apple.filesystems.apfs:__text:FFFFFFF00688D4F0 08 18 00 54              B.HI            loc_FFFFFFF00688D7F0 ; Branch
com.apple.filesystems.apfs:__text:FFFFFFF00688D4F4 EB 36 00 D0+             ADRL            X11, off_FFFFFFF006F6B230 ; "No error."
com.apple.filesystems.apfs:__text:FFFFFFF00688D4F4 6B C1 08 91
com.apple.filesystems.apfs:__text:FFFFFFF00688D4FC 6B 59 74 F8              LDR             X11, [X11,W20,UXTW#3] ; Load from Memory
com.apple.filesystems.apfs:__text:FFFFFFF00688D500 BE 00 00 14              B               loc_FFFFFFF00688D7F8 ; Branch
com.apple.filesystems.apfs:__text:FFFFFFF00688D504                  ; ---------------------------------------------------------------------------
com.apple.filesystems.apfs:__text:FFFFFFF00688D504
com.apple.filesystems.apfs:__text:FFFFFFF00688D504                  loc_FFFFFFF00688D504                    ; CODE XREF: sub_FFFFFFF00688D440+68↑j
com.apple.filesystems.apfs:__text:FFFFFFF00688D504 68 02 00 37              TBNZ            W8, #0, loc_FFFFFFF00688D550 ; Test and Branch Non-Zero
com.apple.filesystems.apfs:__text:FFFFFFF00688D508 68 72 40 F9              LDR             X8, [X19,#0xE0] ; Load from Memory
com.apple.filesystems.apfs:__text:FFFFFFF00688D50C 08 6D 40 F9              LDR             X8, [X8,#0xD8] ; Load from Memory
com.apple.filesystems.apfs:__text:FFFFFFF00688D510 08 81 13 91              ADD             X8, X8, #0x4E0 ; Rd = Op1 + Op2
com.apple.filesystems.apfs:__text:FFFFFFF00688D514 69 6A 40 F9              LDR             X9, [X19,#0xD0] ; Load from Memory
com.apple.filesystems.apfs:__text:FFFFFFF00688D518 29 25 40 B9              LDR             W9, [X9,#0x24] ; Load from Memory
com.apple.filesystems.apfs:__text:FFFFFFF00688D51C 29 05 00 11              ADD             W9, W9, #1 ; Rd = Op1 + Op2
com.apple.filesystems.apfs:__text:FFFFFFF00688D520 6A 86 40 F9              LDR             X10, [X19,#0x108] ; Load from Memory
com.apple.filesystems.apfs:__text:FFFFFFF00688D524 E9 AB 01 A9              STP             X9, X10, [SP,#0x90+var_78] ; Store Pair
com.apple.filesystems.apfs:__text:FFFFFFF00688D528 E8 0B 00 F9              STR             X8, [SP,#0x90+var_80] ; Store to Memory
com.apple.filesystems.apfs:__text:FFFFFFF00688D52C 68 99 FF B0+             ADRL            X8, aApfsMountLivef ; "apfs_mount_livefs"
com.apple.filesystems.apfs:__text:FFFFFFF00688D52C 08 91 1A 91
com.apple.filesystems.apfs:__text:FFFFFFF00688D534 29 50 8B 52              MOV             W9, #0x5A81 ; Rd = Op2
com.apple.filesystems.apfs:__text:FFFFFFF00688D538 E8 27 00 A9              STP             X8, X9, [SP,#0x90+var_90] ; Store Pair
com.apple.filesystems.apfs:__text:FFFFFFF00688D53C 60 99 FF B0+             ADRL            X0, aSDSsD0lldCanTM ; "%s:%d: %ss%d:%.0lld can't mount root fi"...
com.apple.filesystems.apfs:__text:FFFFFFF00688D53C 00 A4 19 91
com.apple.filesystems.apfs:__text:FFFFFFF00688D544 CF 6C FE 97              BL              sub_FFFFFFF006828880 ; Branch with Link
```

ИСПРАВИТЬ НЕИСПРАВИМОЕ: iOS 14.0 и checkm8

Последствия

— загрузка напрямую из DFU невозможна;

— защита от BFU извлечения;

— но нашлись обходные решения, если нельзя загрузиться из DFU, то можно сначала загрузиться в Recovery ;)

SECURE ENCLAVE

— отдельный чип, с отдельными SEPROM и SEPOS;

— хранит GID и UID ключи, отвечающие за всю системную криптографию;

— проверяет собственную прошивку независимо от BootROM и iBoot;

— проверяет пароль разблокировки и биометрию.

SEPROM: Blackbird

— найдена уязвимость в загрузчике Secure Enclave;

— уязвимость невозможно устранить для уже вышедших устройств;

— для эксплуатации уязвимости нужно иметь возможность выполнения произвольного кода на этапе iBoot – например через checkm8;

— сводит на нет все усилия Apple и дает много нового.

SEPROM: Blackbird

Проблемы и последствия

— на данный момент не найдено решения для A11 устройств (iPhone 8, iPhone 8 plus, iPhone X);

— сложность эксплуатации – эксплоит нужно применить из iBoot, значительно усложняет всю цепочку;

— дает возможность загрузить произвольный SEPOS и доступ к защищенной памяти;

— доступ к UID ключам – брутфорс пароля без устройства?

iOS 14.0: objc_direct

— в clang добавлен новый механизм работы с методами в ObjectiveC;

— активно используется в внутренних компонентах iOS 14;

— многие внутренние API стали недоступны без сложного механизма обнаружения адресов;

— разработка джейлбрейков усложняется.

Что дальше?

— возможно выпустим временное решение на основе загрузки в Recovery;

— свой аналог pongoOS;

— решение для SEPOS;

— следите за новостями про поддержку новых Apple-устройств.

БЛАГОДАРЮ
ЗА ВНИМАНИЕ!