Apple lanzó este lunes actualizaciones para iOS, macOS, tvOS y watchOS, con parches de seguridad para múltiples vulnerabilidades, incluyendo una cadena de exploits de fuga remota, además de una serie de problemas críticos en el navegador web Kernel y Safari, que se demostraron por primera vez en la Copa Tianfu celebrada en China hace dos meses.

Rastreada como CVE-2021-30955, el problema podría haber permitido que una aplicación maliciosa ejecutara código arbitrario con privilegios del kernel. Apple dijo que abordó el problema con una *«mejor gestión del estado»*. La falla también afecta a los dispositivos macOS.

> *«El error del núcleo CVE-2021-30955 es el que intentamos a su uso para construir nuestra cadena de jailbreak a distancia, pero no se pudo completar a tiempo»,* dijo el director ejecutivo de Kunlun Lab, @mj0011sec en Twitter.

El equipo de Pangu aprovechó un conjunto de vulnerabilidades del kernel en el concurso de hacking de Tianfu para ingresar a un iPhone 13 Pro con iOS 15, una hazaña que les valió a los hackers de sombrero blanco 330 mil dólares en recompensas en efectivo.

Además de CVE-2021-30955, se han corregido un total de cinco vulnerabilidades de kernel y cuatro IOMobileFrameBuffer (una extensión de kernel para administrar el framebuffer de pantalla) con las últimas actualizaciones:

- CVE-2021-30927 y CVE-2021-30989: Un uso después de un problema gratuito que podría permitir que una aplicación no autorizada ejecute código arbitrario con privilegios del kernel.
- CVE-2021-30937: Una vulnerabilidad de corrupción de memoria que podría permitir que una aplicación no autorizada ejecute código arbitrario con privilegios del kernel.
- CVE-2021-30949: Un problema de corrupción de memoria que podría permitir que una aplicación no autorizada ejecute código arbitrario con privilegios del kernel.
- CVE-2021-30993: Un problema de desbordamiento del búfer que podría permitir que un atacante en una posición de red privilegiada pueda ejecutar código arbitrario.

- CVE-2021-30983: Un problema de desbordamiento del búfer que podría permitir que una aplicación ejecute código arbitrario con privilegios del kernel.
- CVE-2021-30985: Una escritura fuera de los límites que podría permitir que una aplicación ejecute código arbitrario con privilegios de kernel.
- CVE-2021-30991: Un problema de lectura fuera de los límites que podría permitir que una aplicación malintencionada ejecute código arbitrario con privilegios de kernel.
- CVE-2021-30996: Una condición de carrera que podría permitir que una aplicación no autorizada ejecute código arbitrario con privilegios de kernel.

En el frente de macOS, la compañía con sede en Cupertino solucionó un problema con el módulo WiFi (CVE-2021-30938), que un usuario local en el sistema podría explotar para causar una terminación inesperada e incluso leer la memoria del kernel. El gigante tecnológico le dió crédito a Xinru Chi de Pangu Lab por informar la falla.

También se corrigieron siete vulnerabilidades en el componente WebKit: CVE-2021-30934, CVE-2021-30936, CVE-2021-30951, CVE-2021-30952, CVE-2021-30953, CVE-2021-30954 y CVE-2021-30984t, que potencialmente podría resultar en un escenario en el que el procesamiento de contenido web especialmente diseñado puede conducir a la ejecución de código arbitrario.

Además, Apple también resolvió dos problemas que afectaban a las aplicaciones Notes y Password Manager en iOS, que podrían permitir a una persona con acceso físico a un dispositivo iOS acceder a los contactos desde la pantalla de bloqueo y recuperar las contraseñas almacenadas sin ninguna autenticación. Finalmente, se solucionó un error en FaceTime que, de lo contrario, podría haber filtrado información confidencial del usuario por medio de los metadatos de Live Photos.