Unc0ver, una popular herramienta de jailbreak, se ha actualizado para admitir iOS 14.3 y versiones anteriores, haciendo de este modo posible el desbloqueo de casi todos los modelos de iPhone, utilizando una vulnerabilidad que Apple reveló en enero y que fue explotada activamente en la naturaleza.

La última versión, llamada unc0ver v6.0.0, fue lanzada el domingo, según su desarrollador principal Pwn20wnd, ampliando su compatibilidad para hacer jailbreak a cualquier dispositivo que ejecute iOS 11.0 a 14.3, utilizando una vulnerabilidad de kernel.

Rastreada como CVE-2021-1782, la vulnerabilidad de escalada de privilegios en el kernel deriva de una condición de carrera que podría causar que una aplicación maliciosa eleve sus privilegios.

> *«Escribimos nuestro propio exploit basado en CVE-2021-1782 para #unc0ver, para lograr una velocidad y estabilidad óptimas del exploit»,* dijo Pwn20wnd en Twitter.

Desde entonces, Apple abordó la vulnerabilidad como parte de sus actualizaciones de iOS y iPadOS 14.4 lanzadas el 26 de enero de 2021, pero no antes de admitir que el problema pudo haber estado bajo un ataque activo por parte de hackers.

Sin embargo, Apple no reveló qué tan extendido fue el ataque ni reveló las identidades de los atacantes.

El jailbreak, similar al rooteo en Android, implica una escalada de privilegios que funciona al explotar fallas en iOS para otorgar a los usuarios acceso de root y control total sobre sus dispositivos. Al hacerlo, permite a los usuarios de iOS eliminar las restricciones de software impuestas por Apple, permitiendo así el acceso a personalización adicional y aplicaciones prohibidas.

Por su parte, Apple dificulta constantemente el jailbreak de los dispositivos al bloquear su hardware y software por razones de seguridad, lo que según la compañía, ayuda a

contrarrestar los ataques de malware.

Zuk Avraham, CEO de Zimperium, dijo que el jailbreak es *«otro ejemplo más de que los atacantes tienen una ventaja sobre iOS frente a los defensores. Apple debe detener la necesidad de hacer jailbreak al dispositivo en primer lugar y debería permitir el acceso sin necesidad de ejecutar un exploit».*