Apple lanzó este martes actualizaciones para iOS, iPadOS y tvOS, con correcciones para tres vulnerabilidades de seguridad que pueden haber sido explotadas activamente en la naturaleza.

Las tres vulnerabilidades informadas por un investigador anónimo (CVE-2021-1782, CVE-2021-1870 y CVE-2021-1871) podrían haber permitido a un atacante elevar los privilegios y lograr la ejecución remota de código.

Apple no reveló qué tan extendido ha sido el ataque ni las identidades de los atacantes que explotaron las vulnerabilidades activamente.

Aunque el error de escalada de privilegios en el kernel (CVE-2021-1782) se señaló como una condición de carrera que podría hacer que una aplicación maliciosa elevara sus privilegios, las otras dos deficiencias, denominadas como *«problema lógico»*, se descubrieron en el navegador WebKit Engine (CVE-2021-1870 y CVE-2021-1871), lo que permite a un atacante lograr la ejecución de código arbitrario dentro de Safari.

Apple dijo que la condición de carrera y las fallas de WebKit se solucionaron mejorando el bloqueo y las restricciones respectivamente.

Aunque es poco probable que los detalles exactos del exploit que aprovechan las fallas se hagan públicos hasta que los parches se hayan aplicado ampliamente, no parecería una sorpresa si estuvieran encadenados para llevar a cabo ataques de abrevadero contra objetivos potenciales.

Dichos ataques implicarían entregar el código malicioso simplemente visitando un sitio web comprometido que luego se aprovecha de las vulnerabilidades mencionadas anteriormente para escalar sus privilegios y ejecutar comandos arbitrarios para tomar el control del dispositivo.

Las actualizaciones ahora están disponibles para iPhone 6s y posteriores, iPad Air 2 y posteriores, iPad mini 4 y posteriores, iPod touch 7° gen, Apple TV 4K y Apple TV HD.