Tan solo unas semanas después de lanzar parches fuera de banda para iOS, iPadOS, macOS y watchOS, Apple publicó otra actualización de seguridad para iPhone, iPad y Apple Watch para solucionar una debilidad crítica de día cero, que según la compañía, se está explotando activamente.

Rastreada como CVE-2021-1879, la vulnerabilidad se relaciona con una falla de WebKit, que podría permitir a los atacantes procesar contenido web creado con fines malintencionados que puede resultar en ataques universales de secuencias de comandos entre sitios.

> *«Este problema se solucionó mejorando la gestión de la vida útil de los objetos»,* dijo Apple.

Apple reconoció a Clement Lecigne y Billy Leonard, del Threat Analysis Group, de Google, por descubrir e informar sobre el problema. Aunque no se revelaron los detalles de la vulnerabilidad, la compañía dijo que está al tanto de los informes de que CVE-2021-1879 pudo haberse explotado activamente.

Las actualizaciones ya están disponibles para los siguientes dispositivos:

- iOS 12.5.2: iPhone 5s, iPhone 6, iPhone 6 Plus, iPad Air, iPad mini 2, iPad mini 3 y iPoud Touch 6° generación.
- iOS 14.4.2: iPhone 6s y posteriores, iPod Touch 7° generación.
- iPadOS 14.4.2: iPad Pro, iPad Air 2 y posteriores, iPad 5° generación y posteriores, iPad Mini 4 y posteriores.
- watchOS 7.3.3: Apple Watch Series 3 y posteriores.

La última versión llega poco tiempo después de un parche para una falla de webkit separada (CVE-2021-1844) que Apple envió a inicios del mes. En enero de 2021, la compañía resolvió tres vulnerabilidades de día cero; CVE-2021-1782, CVE-2021,1870 y CVE-2021-1871), que permitían a un atacante elevar privilegios y lograr la ejecución remota de código.

Apple también parece estar experimentando formas de entregar actualizaciones de seguridad en iOS de una forma independiente de otras actualizaciones del sistema operativo. iOS 14.4.2 ciertamente parece el tipo de actualización que se beneficiaría de esta función.