Apple lanzó correcciones para una vulnerabilidad crítica de seguridad revelada recientemente, que afecta a dispositivos más antiguos, citando evidencias de explotación activa.

La vulnerabilidad, rastreada como CVE-2022-42856, es una vulnerabilidad de confusión de tipo en el motor del navegador Webkit, que podría resultar en la ejecución de código arbitrario al procesar contenido web creado con fines malintencionados.

Aunque la empresa la abordó originalmente el 30 de noviembre de 2022, como parte de la actualización de iOS 16.1.2, el parche se amplió a un conjunto más grande de dispositivos Apple con iOS 15.7.2, iPadOS 15.7.2, macOS Ventura 13.1, tvOS 16.2 y Safari 16.2.

> *«Apple está al tanto de un informe de que este problema puede haber sido explotado activamente contra versiones de iOS lanzadas antes de iOS 15.1»,* dijo el fabricante de iPhone en un aviso del lunes.

Con ese fin, la última actualización, iOS 12.5.7, está disponible para iPhone 5s, iPhone 6, iPhone 6 Plus, iPad Air, iPad Mini 2, iPad mini 3 y iPod Touch sexta generación.

A Clément Lecigne, del Threat Analysis Group (TAG) de Google, se le atribuye el descubrimiento de la vulnerabilidad, aunque en la actualidad se desconocen los detalles exactos que rodean los intentos de explotación en la naturaleza.

La actualización llega cuando Apple lanza iOS 16.3, iPad OS 16.3, macOS Ventura 13.2, watchOS 9.3 y Safari 16.3, para remediar una larga lista de vulnerabilidades, incluyendo dos errores en Webkit que podrían conducir a la ejecución de código.

macOS Ventura 13.2 también soluciona dos vulnerabilidades de denegación de servicio en ImageIO y Safari, junto con tres vulnerabilidades en el kernel que podrían aprovecharse para filtrar información confidencial, determinar su diseño de memoria y ejecutar código no autorizado con privilegios elevados.

Sin embargo, no todo son correcciones de errores. Las actualizaciones también traen consigo la capacidad de usar claves de seguridad de hardware para bloquear las ID de Apple para una autenticación de dos factores resistente al phishing. También amplían la disponibilidad de Protección de Datos Avanzada fuera de Estados Unidos.