Si usualmente recibes videos por correo electrónico o simplemente los descargas de Internet, cuidado! Podrías ser víctima de un ataque con malware.

Esto porque un archivo de video de aspecto común, especialmente diseñado, puede poner en peligro tu smartphone Android, gracias a una vulnerabilidad crítica de ejecución remota de código que afecta a más de mil millones de dispositivos con sistema operativo Android entre versiones 7.0 y 9.0 (Nougat, Oreo, Pie).

La vulnerabilidad crítica de RCE (CVE-2019-2107) reside en el framework de medios de Android, que de ser explotado, podría permitir que un atacante remoto ejecute código arbitrario en un dispositivo específico.

Para obtener el control total del dispositivo, todo lo que un atacante debe hacer, es engañar al usuario para reproducir un archivo de video específico utilizando la app de reproducción de video nativa de Android.

Aunque Google ya lanzó un parche a inicios de este mes para solucionar dicha vulnerabilidad, aparentemente millones de dispositivos Android siguen esperando la última actualización de seguridad de Android que deberían entregar sus fabricantes.

> *«La vulnerabilidad más grave en esta sección podría permitir que un atacante remoto use un archivo especialmente diseñado para ejecutar código remoto arbitrario dentro del contexto de un proceso privilegiado»,* escribió Google.

Lo que hace que el problema sea aún más preocupante, es que el desarrollador de Android con sede en Alemania, Marcin Kozlowski, subió una prueba de concepto para este ataque a GitHub.

Aunque el PoC compartido por Kozlowski solo bloquea el reproductor de medios, puede ayudar a los posibles atacantes a desarrollar sus propios exploits para lograr RCE en dispositivos específicos.

Sin embargo, se debe tener en cuenta que si dichos videos maliciosos se reciben por medio de una aplicación de mensajería instantánea como WhatsApp o Facebook Messenger, el ataque no funcionará.

Esto se debe a que estos servicios generalmente comprimen videos y vuelven a codificar archivos multimedia que distorsionan el código malicioso incrustado.

La mejor forma de protegerse de este ataque es asegurarse de actualizar su sistema operativo móvil tan pronto como esté disponible el último parche.

Mientras tanto, se recomienda evitar descargar y reproducir videos aleatorios de fuentes no confiables y seguir las prácticas básicas de seguridad.