Investigadores en ciberseguridad han revelado una vulnerabilidad de seguridad corregida que afectaba al decodificador de Monkey's Audio (APE) en smartphones Samsung, la cual podría permitir la ejecución de código malicioso.

El fallo, clasificado como de alta severidad y rastreado como CVE-2024-49415 (puntuación CVSS: 8.1), impacta a dispositivos Samsung que utilizan Android en las versiones 12, 13 y 14.

> *«Un desbordamiento de escritura en `libsaped.so` antes de SMR Dec-2024 Release 1 permite que atacantes remotos ejecuten código arbitrario. La actualización incluye una validación adecuada de los datos de entrada»*, explicó Samsung en un comunicado sobre la vulnerabilidad publicado en diciembre de 2024 como parte de su boletín mensual de seguridad.

Natalie Silvanovich, investigadora de Google Project Zero, quien descubrió y notificó la falla, señaló que esta no requiere interacción del usuario para activarse (conocido como un ataque de tipo «zero-click») y lo describió como una «nueva y curiosa superficie de ataque» bajo ciertas condiciones específicas.

El ataque resulta posible si Google Messages está configurado para usar servicios de comunicación enriquecida (RCS), la configuración predeterminada en los modelos Galaxy S23 y S24, ya que el servicio de transcripción decodifica automáticamente los audios entrantes antes de que el usuario interactúe con ellos.

> *«La función `saped_rec` en `libsaped.so` escribe en un `dmabuf` asignado por el servicio multimedia C2, cuyo tamaño siempre parece ser de 0x120000″,* detalló Silvanovich.
>
> *«Aunque el valor máximo de `blocksperframe` extraído por `libsapedextractor` también está limitado a 0x120000, la función `saped_rec` puede escribir hasta tres*

> *veces el valor de `blocksperframe` si la cantidad de bytes por muestra de entrada es 24. Esto significa que un archivo APE con un tamaño elevado de `blocksperframe` podría causar un desbordamiento considerable en este búfer».*

En un posible escenario de ataque, un actor malintencionado podría enviar un mensaje de audio manipulado a través de Google Messages a un dispositivo objetivo con RCS activado, provocando el bloqueo del proceso de códec de medios («samsung.software.media.c2»).

Además, la actualización de seguridad de diciembre de 2024 de Samsung también soluciona otra vulnerabilidad de alta severidad en SmartSwitch (CVE-2024-49413, puntuación CVSS: 7.1). Este fallo permitía que atacantes locales instalaran aplicaciones maliciosas al aprovechar una verificación incorrecta de las firmas criptográficas.