La Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA), advirtió sobre la explotación activa de una vulnerabilidad de gravedad media que afecta a los dispositivos Samsung.

La vulnerabilidad, rastreada como CVE-2023-21492 (puntaje CVSS: 4.4), afecta a dispositivos Samsung seleccionados que ejecutan las versiones 11, 12 y 13 de Android.

La compañía de Corea del Sur describió el problema como una falla de divulgación de información que podría ser explotada por un atacante privilegiado para eludir las protecciones de aleatorización del diseño del espacio de direcciones (ASLR).

ASLR es una técnica de seguridad diseñada para evitar la corrupción de la memoria y las fallas en la ejecución del código ocultando la ubicación de un ejecutable en la memoria de un dispositivo.

Samsung, en un aviso publicado este mes, dijo que fue *«notificado de que había existido un exploit para este problema»,* y agregó que se reveló de forma privada a la compañía el 17 de enero de 2023.

Actualmente no se conocen otros detalles sobre cómo se explota la vulnerabilidad, pero en el pasado los vendedores comerciales de spyware han utilizado las vulnerabilidades en los teléfonos Samsung para implementar software malicioso.

En agosto de 2020, Google Project Zero también demostró un ataque MMS remoto sin clic que aprovechó dos vulnerabilidades de sobrescritura de búfer en la biblioteca qmg de Quram (SVE-2020-16747 y SVE-2020-17675) para derrotar a ASLR y lograr la ejecución del código.

A la luz del abuso activo, CISA agregó la deficiencia a su catálogo de vulnerabilidades conocidas explotadas (KEV), junto con dos vulnerabilidades de Cisco IOS (CVE-2004-1464 y CVE-2016-6415), instando a las agencias de la Rama Ejecutiva Civil Federal (FCEB) a aplicar parches antes del 9 de junio de 2023.

La semana pasada, CISA también agregó siete vulnerabilidades al catálogo de KEV, la más antigua de las cuales es un error de 13 años que afecta a Linux (CVE-2010-3904) que permite que un atacante local sin privilegios pueda escalar sus privilegios a root.