Google lanzó parches de seguridad mensuales para Android con correcciones para 37 vulnerabilidades en distintos componentes, una de las cuales es una corrección para vulnerabilidad del kernel de Linux explotada activamente, que se dio a conocer a inicios de 2022.

Registrada como CVE-2021-22600, con puntuación CVSS de 7.8, la vulnerabilidad está clasificada como alta en gravedad y podría ser explotada por un usuario local para aumentar los privilegios o denegar el servicio.

El problema se relaciona con una vulnerabilidad de doble liberación que reside en la implementación del protocolo de red Packet en el kernel de Linux, que podría causar daños en la memoria, lo que podría provocar una denegación de servicio o la ejecución de código arbitrario.

Los parches fueron lanzados por distintas distribuciones de Linux, incluyendo Debian, Red Hat, SUSE y Ubuntu en enero de 2022.

«Hay indicios de que CVE-2021-22600 puede estar bajo una explotación limitada y dirigida», dijo Google en su Boletín de Seguridad de Android de mayo de 2022. Aún no se conocen los detalles sobre la naturaleza de los ataques.

Cabe mencionar que la vulnerabilidad también fue agregada por la Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA) a su Catálogo de Vulnerabilidades Explotadas Conocidas, a partir del mes pasado en función de la evidencia de explotación activa.

También se corrigieron como parte de los parches de este mes otros tres errores en el núcleo, así como 18 fallas de alta gravedad y una de gravedad crítica en los componentes de MediaTek y Qualcomm.