Qualcomm lanzó el martes parches para abordar múltiples vulnerabilidades de seguridad en sus conjuntos de chips, algunas de las cuales, podrían explotarse para causar divulgación de información y corrupción de memoria.

Las cinco vulnerabilidades, rastreadas desde CVE-2022-40516 hasta CVE-2022-40520, también afectan a las computadoras portátiles Lenovo ThinkPad X13s, lo que llevó al fabricante chino de PC a publicar actualizaciones de BIOS para corregir los problemas.

Las vulnerabilidades se describen como:

- CVE-2022-40516, CVE-2022-40517 y CVE-2022-40520 (Puntaje CVSS: 8.4): Corrupción de memoria en Core debido a un desbordamiento de búfer basado en pila
- CVE-2022-40518 y CVE-2022-40519 (puntaje CVSS: 6.8): Divulgación de información debido a una sobrelectura del búfer en Core

Las vulnerabilidades de desbordamiento de búfer basadas en la pila pueden tener efectos graves, como daños en los datos, bloqueos del sistema y ejecución de código arbitrario. Las lecturas excesivas de búfer, por otro lado, pueden usarse como armas para leer memoria fuera de los límites, lo que lleva a la exposición de datos secretos.

La explotación exitosa de las vulnerabilidades podría permite que un hacker local con privilegios elevados provoque daños en la memoria o filtre información confidencial, dijo Lenovo en una alerta publicada el martes.

Lenovo también corrigió cuatro vulnerabilidades de lectura excesiva de búfer en el BIOS ThinkPad X13 que podrían conducir a la divulgación de información. Los defectos se rastrean como CVE-2022-4432, CVE-2022-4433, CVE-2022-4434 y CVE-2022-4435.

Se recomienda a los usuarios de ThinkPad X13 que actualicen el BIOS a la versión 1.47 (N3HET75W) o posterior. A la empresa de seguridad de firmware Binarly se le atribuye el descubrimiento y la notificación de las nueve vulnerabilidades.

El boletín de seguridad de enero de 2023 de Qualcomm elimina otras 17 vulnerabilidades, incluyendo un error crítico de corrupción de memoria en el componente automotriz (CVE-2022-33219, puntaje CVSS: 9.3) que surge como resultado de una vulnerabilidad de desbordamiento de búfer.