Una serie de vulnerabilidades de seguridad de firmware descubiertas en las computadoras portátiles de gama alta orientadas a los negocios de HP, siguen sin parches en algunos dispositivos aún pasados varios meses de la divulgación pública.

Binarly, que reveló por primera vez los detalles de las vulnerabilidades en la conferencia Black Hat USA a mediados de agosto de 2022, dijo que las vulnerabilidades *«no pueden ser detectadas por los sistemas de monitoreo de integridad del firmware debido a las limitaciones de la medición del Módulo de Plataforma Segura (TPM)».*

Las fallas de firmware pueden tener implicaciones graves, ya que un atacante puede abusar de ellas para lograr una persistencia a largo plazo en un dispositivo de forma que pueda sobrevivir a los reinicios y evadir las protecciones de seguridad tradicionales del sistema operativo.

Las vulnerabilidades de alta gravedad identificadas por Binarly afectan a los dispositivos HP EliteBook y se refieren a un caso de corrupción de memoria en el módulo de administración del sistema (SMM) del firmware, lo que permite la ejecución de código arbitrario con los privilegios más altos:

- CVE-2022-23920 (puntaje CVSS: 8.2): Desbordamiento del búfer basado en pila
- CVE-2022-31640 (puntaje CVSS: 7.5): Validación de entrada incorrecta
- CVE-2022-31641 (puntaje CVSS: 7.5): Validación de entrada incorrecta
- CVE-2022-31644 (puntaje CVSS: 7.5): Escritura fuera de los límites
- CVE-2022-31645 (puntaje CVSS: 8.2): Escritura fuera de ls límites
- CVE-2022-31646 (puntaje CVSS: 8.2): Escritura fuera de los límites

Tres de los errores (CVE-2022-23930, CVE-2022-31640 y CVE-2022-31641) se notificaron a HP en julio de 2021, con las tres vulnerabilidades restantes (CVE-2022-31644, CVE-2022-31645 y CVE-2022-31646) informadas en abril de 2022.

Cabe mencionar que CVE-2022-23930 también es una de las 16 vulnerabilidades que se señalaron anteriormente en febrero como un impacto en varios modelos empresariales de

HP.

SMM, también llamado *«Ring-2»*, es un modo de propósito especial utilizado por el firmware (es decir, UEFI) para manejar funciones de todo el sistema, como administración de energía, interrupciones de hardware u otro código diseñado por el fabricante de equipos originales (OEM).

Las vulnerabilidades identificadas en el componente SMM pueden, por lo tanto, actuar como un lucrativo vector de ataque para que los atacantes realicen actividades maliciosas con mayores privilegios que los del sistema operativo.

Aunque HP lanzó mitigaciones para abordar las vulnerabilidades en marzo y agosto, el proveedor aún tiene que impulsar los parches para todos los modelos afectados, lo que podría exponer a los clientes al riesgo de ataques cibernéticos.

> *«En muchos casos, el firmware es un único punto de falla entre todas las capas de la cadena de suministro y el dispositivo final del cliente. Arreglar las vulnerabilidades de un solo proveedor no es suficiente»*, dijo Binarly.

> *«Como resultado de la complejidad de la cadena de suministro de firmware, existen brechas que son difíciles de cerrar en el extremo de la fabricación, ya que involucra problemas que escapan al control de los proveedores de dispositivos».*

La divulgación también llega cuando el fabricante de computadoras implementó la semana pasada correcciones para una vulnerabilidad de escalada de privilegios (CVE-2022-38395, puntaje CVSS: 8.2) en su software de solución de problemas Support Assistant.

> *«Es posible que un atacante explote la vulnerabilidad de secuestro de DLL y eleve*

> *los privilegios cuando Fusion lanza HP Performance Tune-up»,* dijo la compañía.