Se descubrieron tres vulnerabilidades de seguridad de interfaz de firmware extensible unificada (UEFI) de alto impacto, que afectan a varios modelos de portátiles de consumo de Lenovo, lo que permite a los atacantes implementar y ejecutar implantes de firmware en los dispositivos afectados.

Rastreadas como CVE-2021-3970, CVE-2021-3971 y CVE-2021-3972, las dos últimas vulnerabilidades *«afectan los controladores de firmware originalmente destinados a usarse solo durante el proceso de fabricación de las computadoras portátiles de consumo de Lenovo»,* dijo el investigador de ESET, Martin Smolár.

> *«Desafortunadamente, también se incluyeron por error en las imágenes del BIOS de producción sin desactivarlas correctamente»,* agregó Smolár.

La explotación exitosa de las vulnerabilidades podría permitir que un atacante deshabilite las protecciones flash SPI o el arranque seguro, otorgando efectivamente al adversario la capacidad de instalar malware persistente que pueda sobrevivir a los reinicios del sistema.

CVE-2021-3970, por otro lado, se relaciona con un caso de corrupción de memoria en el Modo de Administración del Sistema (SMM) de la compañía, lo que llevó a la ejecución de código malicioso con los privilegios más altos.

Las tres fallas se informaron a la compañía el 11 de octubre de 2021, después de lo cual se emitieron parches el 12 de abril de 2022. Un resumen de las vulnerabilidades se describe a continuación:

- CVE-2021-3970: Una vulnerabilidad potencial en LenovoVariable SMI Handler, debido a una validación insuficiente en algunos modelos de portátiles Lenovo puede permitir que un atacante con acceso local y privilegios elevados ejecute código arbitrario.

- CVE-2021-3971: Una posible vulnerabilidad de un controlador utilizado durante los procesos de fabricación más antiguos en algunos dispositivos portátiles Lenovo de consumo que se incluyó por error en la imagen del BIOS, podría permitir que un atacante con privilegios elevados modifique la región de protección del firmware mediante la modificación de una variable NVRAM.
- CVE-2021-3972: Una posible vulnerabilidad de un controlador utilizado durante el proceso de fabricación en algunos dispositivos portátiles Lenovo de consumo que no se desactivó por error, puede permitir que un atacante con privilegios elevados modifique la configuración de arranque seguro modificando una variable NVRAM.

Las vulnerabilidades, que impactan a Lenovo Flex, IdeaPads, Legion, series V14, V15 y V17, y portátiles Yoga, se suman a la revelación de hasta 50 vulnerabilidades de firmware UEFI en InsydeH2O, HP y Dell de Insyde Software desde inicios de año.

En la lista se incluyen seis vulnerabilidades graves en el firmware HP que afectan a las computadoras portátiles y de escritorio, que de ser explotadas exitosamente, podrían permitir a los hackers escalar localmente a los privilegios de SMM y desencadenar una condición de denegación de servicio (DoS).

> *«Las amenazas UEFI pueden ser extremadamente sigilosas y peligrosas. Se ejecutan temprano en el proceso de arranque, antes de transferir el control al sistema operativo, lo que significa que pueden eludir casi todas las medidas de seguridad y mitigaciones más altas en la pila que podrían evitar que se ejecuten las cargas útiles de su sistema operativo»,* dijo Smolár.