El fabricante de productos electrónicos de consumo Lenovo, lanzó este martes correcciones para contener tres vulnerabilidades de seguridad en su firmware UEFI, que afectan a más de 70 modelos de productos.

> *«Las vulnerabilidades pueden explotarse para lograr la ejecución de código arbitrario en las primeras fases del arranque de la plataforma, lo que posiblemente permita a los atacantes secuestrar el flujo de ejecución del sistema operativo y deshabilitar algunas funciones de seguridad importantes»,* dijo la compañía ESET.

Registradas como CVE-2022-1890, CVE-2022-1891 y CVE-2022-1892, las tres vulnerabilidades se relacionan con vulnerabilidades de desbordamiento de búfer que Lenovo describió como conducentes a una escalada de privilegios en los sistemas afectados. A Martin Smolár de ESET se le atribuye haber informado las fallas.

Las vulnerabilidades se derivan de una validación insuficiente de una variable NVRAM llamada *«DataSize»* en tres controladores distintos, ReadyBootDxe, SystemLoadDefaultDxe y SystemBootManagerDxe, lo que lleva a un desbordamiento de búfer que podría convertirse en un arma para lograr la ejecución del código.

Esta es la segunda vez que Lenovo se ha movido para abordar vulnerabilidades de seguridad de UEFI desde inicios de 2022. En abril, la empresa corrigió tres vulnerabilidades (CVE-2021-3970, CVE-2021-3971 y CVE-2021-3972), también descubiertas por Smolár, que podrían haber sido objeto de abuso para implementar y ejecutar implantes de firmware.

Se recomienda a los usuarios de los dispositivos afectados que actualicen su firmware a la última versión para mitigar posibles amenazas.