Los expertos en ciberseguridad han revelado detalles sobre una falla de seguridad, ahora solucionada, en el firmware Phoenix SecureCore UEFI que afecta a varias familias de procesadores Intel Core tanto de escritorio como móviles.

Catalogada como CVE-2024-0762 (puntuación CVSS: 7.5), la vulnerabilidad «UEFIcanhazbufferoverflow» ha sido descrita como un desbordamiento de búfer que surge del uso de una variable insegura en la configuración del Módulo de Plataforma Confiable (TPM), lo que podría permitir la ejecución de código malicioso.

> *«La vulnerabilidad permite a un atacante local elevar privilegios y ejecutar código dentro del firmware UEFI durante el tiempo de ejecución,»* explicó la empresa de seguridad de la cadena de suministro Eclypsium.
>
> *«Este tipo de explotación a bajo nivel es característica de puertas traseras en firmware (por ejemplo, BlackLotus) que se están observando cada vez más. Estos implantes permiten a los atacantes mantener una persistencia continua en un dispositivo y, a menudo, evadir las medidas de seguridad de nivel superior que se ejecutan en el sistema operativo y en las capas de software.»*

Tras una divulgación responsable, la vulnerabilidad fue corregida por Phoenix Technologies en abril de 2024. El fabricante de PC Lenovo también ha lanzado actualizaciones para solucionar esta falla desde el mes pasado.

> *«Esta vulnerabilidad afecta a dispositivos que usan el firmware Phoenix SecureCore en familias selectas de procesadores Intel, incluyendo AlderLake, CoffeeLake, CometLake, IceLake, JasperLake, KabyLake, MeteorLake, RaptorLake, RocketLake y TigerLake,»* afirmó el desarrollador del firmware.

UEFI, sucesor de BIOS, es el firmware de la placa base utilizado durante el arranque para inicializar los componentes de hardware y cargar el sistema operativo a través del gestor de arranque.

El hecho de que UEFI sea el primer código que se ejecuta con los más altos privilegios lo ha convertido en un objetivo atractivo para los atacantes que buscan desplegar bootkits e implantes de firmware que pueden subvertir los mecanismos de seguridad y mantener la persistencia sin ser detectados.

Esto también implica que las vulnerabilidades descubiertas en el firmware UEFI pueden representar un grave riesgo para la cadena de suministro, ya que pueden afectar a muchos productos y proveedores diferentes simultáneamente.

> *«El firmware UEFI es uno de los códigos de mayor valor en los dispositivos modernos, y cualquier compromiso de ese código puede dar a los atacantes control total y persistencia en el dispositivo,»* señaló Eclypsium.

Este desarrollo se produce casi un mes después de que la empresa revelara una falla similar de desbordamiento de búfer no corregida en la implementación UEFI de HP, que afecta al HP ProBook 11 EE G1, un dispositivo que alcanzó el estado de fin de vida útil (EoL) en septiembre de 2020.

También sigue a la revelación de un ataque de software llamado TPM GPIO Reset, que podría ser explotado por los atacantes para acceder a secretos almacenados en disco por otros sistemas operativos o socavar controles protegidos por el TPM, como el cifrado de disco o las protecciones de arranque.