Se revelaron nuevas vulnerabilidades de seguridad en Dell BIOS, que de ser explotadas, podrían conducir a la ejecución de código en sistemas vulnerables, uniéndose a las vulnerabilidades de firmware descubiertas recientemente en InsydeH20 de Insyde Software y HP Unified Extensible Firmware Interface (UEFI).

Rastreadas como CVE-2022-24415, CVE-2022-24416, CVE-2022-24419, CVE-2022-24420 y CVE-2022-24421, las vulnerabilidades de alta gravedad tienen una calificación de 8.2 sobre 10 en el sistema de puntuación CVSS.

> *«La explotación activa de todas las vulnerabilidades descubiertas no puede ser detectada por los sistemas de monitoreo de integridad del fimware debido a las limitaciones de la medición del módulo de la plataforma segura (TPM)»,* dijo la compañía de seguridad de firmware, Binarly, que descubrió las últimas tres vulnerabilidades mencionadas.

> *«Las soluciones de atestación del estado del dispositivo remoto no detectarán los sistemas afectados debido a las limitaciones de diseño en la visibilidad del tiempo de ejecución del firmware».*

Todas las vulnerabilidades se relacionan con las vulnerabilidades de validación de entrada incorrecta que afectan el modo de administración del sistema (SSM) del firmware, lo que permite que un atacante local autenticado aproveche la interrupción de administración del sistema (SMI) para lograr la ejecución de código arbitrario.

El modo de administración del sistema se refiere a un modo de CPU de propósito especial en microcontroladores x86 que está diseñado para manejar funciones de todo el sistema, como administración de energía, control de hardware del sistema, monitoreo térmico y otro código desarrollado por el fabricante propietario.

Cada vez que se solicita una de estas operaciones, se invoca una interrupción no enmascarable (SMI) en tiempo de ejecución, que ejecuta el código SMM instalado por el BIOS. Debido a que el código SMM se ejecuta en el nivel de privilegios más alto y es invisible para el sistema operativo subyacente, el método propicia el abuso para implementar implantes de firmware persistentes.

Varios productos de Dell, incluidos Alienware, Inspiron, Vostro y Edge Gateway 3000 Series, se ven afectados, y el fabricante de PC con sede en Texas recomienda a los clientes que actualicen su BIOS lo antes posible.

> *«El descubrimiento continuo de estas vulnerabilidades demuestra lo que describimos como 'fallas repetibles' en torno a la falta de saneamiento de entrada, o en general, prácticas de codificación inseguras»,* dijeron los investigadores de Binarly.

> *«Estas fallas son una consecuencia directa de la complejidad de la base de código o la compatibilidad con componentes heredados que reciben menos atención de seguridad, pero que aún se implementan ampliamente en el campo. En muchos casos, la misma vulnerabilidad se puede corregir en múltiples iteraciones y aún así, la complejidad de la superficie de ataque deja brechas abiertas para la explotación maliciosa».*