Determinados modelos de placas base de fabricantes como ASRock, ASUSTeK Computer, GIGABYTE y MSI se ven afectados por una vulnerabilidad de seguridad que los deja expuestos a ataques de acceso directo a memoria (DMA) durante las primeras fases del arranque en arquitecturas que utilizan Unified Extensible Firmware Interface (UEFI) y una unidad de gestión de memoria de entrada/salida (IOMMU).

UEFI e IOMMU están concebidos para establecer una base de seguridad sólida y evitar que los periféricos realicen accesos no autorizados a la memoria, garantizando que los dispositivos con capacidad DMA no puedan manipular ni inspeccionar la memoria del sistema antes de que el sistema operativo se cargue.

La falla, identificada por Nick Peterson y Mohamed Al-Sharifi de Riot Games en determinadas implementaciones de UEFI, está relacionada con una discrepancia en el estado de la protección DMA. Aunque el firmware indica que la protección DMA está activa, no logra configurar ni habilitar correctamente la IOMMU durante la fase crítica del arranque.

"Esta brecha permite que un dispositivo malicioso con capacidad DMA y acceso físico, a través de Peripheral Component Interconnect Express (PCIe), pueda leer o modificar la memoria del sistema antes de que se establezcan las protecciones a nivel del sistema operativo", señaló el CERT Coordination Center (CERT/CC) en un aviso de seguridad.

"Como consecuencia, los atacantes podrían acceder a información sensible almacenada en memoria o influir en el estado inicial del sistema, comprometiendo así la integridad del proceso de arranque."

La explotación exitosa de esta vulnerabilidad podría permitir que un atacante con acceso físico habilite la inyección de código antes del arranque en sistemas afectados que ejecuten firmware sin parches, además de acceder o alterar la memoria del sistema mediante transacciones DMA mucho antes de que se carguen el kernel del sistema operativo y sus mecanismos de seguridad.

Las vulnerabilidades que hacen posible eludir la protección de memoria durante el arranque

temprano se enumeran a continuación:

- CVE-2025-14304 (puntuación CVSS: 7.0) – Vulnerabilidad por fallo en el mecanismo de protección que afecta a placas base ASRock, ASRock Rack y ASRock Industrial que utilizan chipsets Intel de las series 500, 600, 700 y 800.
- CVE-2025-11901 (puntuación CVSS: 7.0) – Vulnerabilidad por fallo en el mecanismo de protección que impacta a placas base ASUS con chipsets Intel Z490, W480, B460, H410, Z590, B560, H510, Z690, B660, W680, Z790, B760 y W790.
- CVE-2025-14302 (puntuación CVSS: 7.0) – Vulnerabilidad por fallo en el mecanismo de protección que afecta a placas base GIGABYTE con chipsets Intel Z890, W880, Q870, B860, H810, Z790, B760, Z690, Q670, B660, H610 y W790, así como a chipsets AMD X870E, X870, B850, B840, X670, B650, A620, A620A y TRX50 (la corrección para TRX50 está prevista para el primer trimestre de 2026).
- CVE-2025-14303 (puntuación CVSS: 7.0) – Vulnerabilidad por fallo en el mecanismo de protección que afecta a placas base MSI que utilizan chipsets Intel de las series 600 y 700.

Dado que los fabricantes afectados están publicando actualizaciones de firmware para corregir la secuencia de inicialización de la IOMMU y reforzar la protección DMA durante todo el proceso de arranque, es fundamental que los usuarios finales y administradores las apliquen tan pronto como estén disponibles para mantenerse protegidos frente a esta amenaza.

“En entornos donde el acceso físico no puede controlarse por completo o no es confiable, la aplicación oportuna de parches y el cumplimiento de las mejores prácticas de seguridad de hardware resultan especialmente críticos”, indicó CERT/CC. *“Dado que la IOMMU también desempeña un papel fundamental en el aislamiento y la delegación de confianza en entornos virtualizados y en la nube, esta falla subraya la importancia de garantizar una configuración correcta del firmware incluso en sistemas que normalmente no se utilizan en centros de datos.”*

Actualización

Riot Games, en una publicación independiente, explicó que la vulnerabilidad crítica podría explotarse para la inyección de código, destacando que el estado privilegiado asociado a la secuencia temprana de arranque puede manipularse antes de que el sistema operativo active sus controles de seguridad.

"Este problema permitió que trampas de hardware pudieran inyectar código sin ser detectadas, incluso cuando las configuraciones de seguridad del sistema anfitrión parecían estar habilitadas", afirmó Al-Sharifi, describiéndolo como un problema de *"Sleeping Bouncer"*.

Aunque la Protección DMA Pre-Arranque está diseñada para impedir accesos DMA maliciosos a la memoria del sistema mediante la IOMMU desde las primeras etapas del arranque, la vulnerabilidad surge porque el firmware señaliza incorrectamente al sistema operativo que esta función está plenamente activa, cuando en realidad no inicializa correctamente la IOMMU durante el arranque temprano.

"Esto significaba que, aunque las opciones de 'Pre-Boot DMA Protection' parecían estar habilitadas en la BIOS, la implementación subyacente del hardware no estaba inicializando completamente la IOMMU durante los primeros segundos del proceso de arranque", añadió Al-Sharifi. *"En esencia, el 'guardia de seguridad' del sistema parecía estar en su puesto, pero en realidad estaba dormido en la silla. Para cuando el sistema termina de cargarse, no puede tener la certeza absoluta de que no se haya inyectado código que comprometa la integridad a través de DMA."*

Esta breve ventana de explotación puede allanar el camino para una *"trampa de hardware sofisticada"* que logre infiltrarse, obtener privilegios elevados y ocultarse sin generar alertas. *"Al cerrar esta brecha previa al arranque, estamos neutralizando toda una clase de trampas que antes eran prácticamente intocables y elevando significativamente el costo del juego desleal"*, señaló Riot Games.

Si bien la vulnerabilidad se ha presentado desde la perspectiva del sector de los videojuegos, el riesgo de seguridad se extiende a cualquier ataque que pueda aprovechar el acceso físico

para inyectar código malicioso.