Un grupo de académicos de KU Leuven y de la University of Birmingham ha mostrado una nueva vulnerabilidad llamada Battering RAM que permite eludir las defensas más recientes en procesadores de nube de Intel y AMD.

"Construimos un interposer sencillo, de unos 50 dólares, que se coloca discretamente en la ruta de la memoria, comportándose de forma transparente durante el arranque y superando todas las comprobaciones de confianza," explicaron los investigadores Jesse De Meulemeester, David Oswald, Ingrid Verbauwhede y Jo Van Bulck en la web donde difundieron sus hallazgos. *"Más tarde, con solo accionar un interruptor, nuestro interposer se vuelve malicioso y redirige silenciosamente direcciones protegidas hacia ubicaciones controladas por el atacante, permitiendo la corrupción o la reproducción de memoria cifrada."*

Battering RAM compromete las funciones de seguridad de hardware Intel Software Guard Extensions (SGX) y AMD Secure Encrypted Virtualization con Secure Nested Paging (SEV-SNP), que están diseñadas para mantener los datos del cliente cifrados en memoria y protegidos durante su uso.

La falla afecta a todos los sistemas que emplean memoria DDR4, y en particular a aquellos que dependen de cargas de trabajo de *confidential computing* en entornos de nube pública para proteger datos frente al proveedor de servicios en la nube mediante control de acceso a nivel de hardware y cifrado de memoria.

En resumen, el ataque usa un interposer DDR4 hecho a medida y de bajo coste para desviar de forma sigilosa direcciones físicas y obtener acceso no autorizado a regiones de memoria protegida. El interposer utiliza conmutadores analógicos simples para manipular activamente las señales entre CPU y memoria, y puede construirse por menos de $50.

En plataformas Intel, Battering RAM logra lecturas arbitrarias del texto sin cifrar de la víctima o escribe texto sin cifrar dentro de enclaves de la víctima; en sistemas AMD, el ataque puede emplearse para sortear recientes mitigaciones de firmware contra BadRAM (documentadas por los mismos investigadores en diciembre de 2024) e introducir puertas traseras arbitrarias

en la máquina virtual sin levantar sospechas.

La explotación exitosa de la vulnerabilidad permitiría a un proveedor de infraestructura en la nube deshonesto o a un insider con acceso físico limitado comprometer la atestación remota y posibilitar la inserción de puertas traseras arbitrarias en cargas de trabajo protegidas.

La vulnerabilidad fue reportada a los fabricantes a comienzos de este año; Intel, AMD y Arm respondieron que los ataques físicos actualmente se consideran fuera de alcance. No obstante, los investigadores remarcaron que defenderse de Battering RAM exigiría rediseñar de forma fundamental el propio cifrado de memoria.

"Battering RAM revela las limitaciones fundamentales de los diseños escalables de cifrado de memoria que usan actualmente Intel y AMD, los cuales prescinden de comprobaciones criptográficas de frescura a favor de tamaños mayores de memoria protegida," añadieron. *"Battering RAM [...] es capaz de introducir alias de memoria de forma dinámica en tiempo de ejecución. Como resultado, Battering RAM puede eludir las comprobaciones de alias realizadas por Intel y AMD en el arranque."*

La divulgación llega en un contexto en el que AMD publicó mitigaciones para ataques denominados Heracles y Relocate-Vote, revelados por la University of Toronto y ETH Zürich respectivamente, que podían filtrar datos sensibles desde entornos en la nube y máquinas virtuales confidenciales que confían en la tecnología SEV-SNP de AMD mediante la actuación de un hipervisor malicioso.

"El sistema permite al hipervisor mover datos para gestionar la memoria de forma eficiente," dijo David Lie, director del Schwartz Reisman Institute (SRI) de la University of Toronto. *"Así, cuando los datos se reubican, el hardware de AMD los descifra desde la ubicación antigua y los vuelve a cifrar para la nueva ubicación. Pero descubrimos que repitiendo esto una y otra vez, un hipervisor malicioso puede aprender patrones recurrentes en los datos, lo que podría derivar en brechas de privacidad."*

El mes pasado, investigadores de ETH Zürich también mostraron que una optimización de

CPU conocida como *stack engine* puede ser abusada como canal lateral para ataques que provocan fugas de información. Se ha desarrollado una prueba de concepto (PoC) para máquinas AMD Zen 5, aunque se cree que todos los modelos poseen esta "característica de hardware que se puede explotar".

El hallazgo de Battering RAM también sigue a un informe de investigadores de la Vrije Universiteit Amsterdam sobre una técnica de ataque nueva y realista denominada L1TF Reloaded, que combina L1 Terminal Fault (también conocido como Foreshadow) y gadgets Half-Spectre (patrones de código incompletos similares a Spectre) para filtrar memoria de máquinas virtuales que se ejecutan en servicios de nube pública.

"L1TF es una vulnerabilidad de CPU que permite a una VM (atacante) leer especulativamente cualquier dato residiendo en la caché de datos L1 local al núcleo —incluyendo datos a los que la VM no debería tener acceso," explicaron los investigadores de VUSec. *"A grandes rasgos, L1TF Reloaded abusa de esto para obtener una primitiva de lectura arbitraria de RAM."*

Google, que proporcionó a los investigadores un nodo de inquilino exclusivo para realizar la investigación de forma segura sin afectar potencialmente a otros clientes, otorgó una recompensa (bug bounty) de $151,515 y *"aplicó correcciones a los activos afectados."* Amazon declaró que la vulnerabilidad L1TF Reloaded no afecta a los datos de los clientes de AWS que se ejecutan en el AWS Nitro System o Nitro Hypervisor.

Spectre, que salió a la luz a principios de 2018, sigue causando problemas en CPUs modernas mediante distintas variantes. Hace apenas dos semanas, académicos de ETH Zürich idearon un nuevo ataque denominado VMScape (CVE-2025-40300, puntuación CVSS: 6.5) que rompe los límites de virtualización en CPUs AMD Zen y procesadores Intel Coffee Lake.

Descrito como un ataque de inyección de objetivo de rama tipo Spectre (Spectre-BTI) orientado a la nube, explota huecos de aislamiento entre host y guest en modos usuario y supervisor para filtrar memoria arbitraria desde un proceso QEMU sin modificar. Se ha introducido una corrección por software en el kernel de Linux para contrarrestar la primitiva de ataque vBTI (BTI entre virtualizaciones).

"VMScape puede filtrar la memoria del proceso QEMU a una velocidad de 32 B/s en AMD Zen 4," afirmaron los autores. *"Usamos VMScape para localizar datos secretos y filtrarlos, todo en 772 s, extrayendo como ejemplo la clave criptográfica usada para cifrar/descifrar discos."*