Investigadores del ETH Zürich han identificado una nueva vulnerabilidad de seguridad que, según ellos, afecta a todos los procesadores modernos de Intel y permite la filtración de datos sensibles desde la memoria, demostrando que el problema conocido como *Spectre* sigue representando una amenaza para los sistemas informáticos incluso después de más de siete años.

> La vulnerabilidad, denominada *Branch Privilege Injection (BPI)*, *"puede ser explotada para manipular los cálculos de predicción de la CPU (unidad central de procesamiento) con el fin de obtener acceso no autorizado a información perteneciente a otros usuarios del procesador",* explicó ETH Zürich.

Kaveh Razavi, líder del Grupo de Seguridad Informática (COMSEC) y uno de los autores del estudio, señaló que la falla afecta a todos los procesadores Intel, lo que podría permitir a atacantes malintencionados leer tanto la caché del procesador como la memoria activa perteneciente a otro usuario que utilice el mismo chip.

El ataque se basa en una técnica conocida como *Branch Predictor Race Conditions (BPRC)*, que se produce cuando el procesador alterna entre cálculos de predicción correspondientes a usuarios con distintos niveles de privilegio. Esto genera una situación en la que un atacante sin privilegios podría eludir las protecciones de seguridad y acceder a información confidencial de un proceso con mayores permisos.

Intel ha lanzado actualizaciones de microcódigo para mitigar esta vulnerabilidad, la cual ha sido registrada bajo el identificador CVE-2024-45332 (puntuación CVSS v4: 5.7).

"Divulgación de información sensible causada por el estado compartido del predictor microarquitectónico, el cual afecta la ejecución transitoria en los predictores de bifurcación indirecta de algunos procesadores Intel, podría permitir a un usuario autenticado habilitar potencialmente la exposición de datos mediante acceso local", indicó Intel en una alerta publicada el 13 de mayo.

Esta revelación coincide con otra investigación del grupo *Systems and Network Security* (VUSec) de la Universidad Vrije de Ámsterdam, que ha descrito una nueva categoría de ataques *Spectre v2* denominada *Training Solo*.

"Los atacantes pueden redirigir de forma especulativa el flujo de control dentro del mismo dominio (por ejemplo, el núcleo del sistema) y filtrar información cruzando los límites de privilegios, reactivando así escenarios clásicos de Spectre v2 sin depender de entornos restringidos como eBPF", señaló VUSec.

Los ataques de hardware, registrados como CVE-2024-28956 y CVE-2025-24495, pueden utilizarse para extraer memoria del núcleo en procesadores Intel a una velocidad de hasta 17 Kb/s. El estudio concluye que estos ataques *"pueden romper completamente el aislamiento entre dominios y volver a habilitar ataques tradicionales Spectre v2 entre usuarios, máquinas virtuales, e incluso entre una máquina virtual y su anfitrión".*

- CVE-2024-28956 (puntuación CVSS v4: 5.7) – *Indirect Target Selection (ITS)*, afecta a Intel Core de 9ª a 11ª generación, así como a procesadores Intel Xeon de 2ª y 3ª generación, entre otros.
- CVE-2025-24495 (puntuación CVSS v4: 6.8) – Vulnerabilidad relacionada con la unidad de predicción de bifurcaciones (*Lion Cove BPU*), presente en procesadores Intel con núcleos Lion Cove.

Si bien Intel ya ha publicado actualizaciones de microcódigo para mitigar estas fallas, AMD ha actualizado su documentación sobre *Spectre* y *Meltdown* para recalcar específicamente el riesgo asociado al uso del filtro clásico de paquetes de Berkeley (*cBPF*).