Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

NUEVO ATAQUE LLAMADO PHOENIX ROWHAMMER ROMPE LA SEGURIDAD DE LA MEMORIA DDR5 EN SEGUNDOS

16/ 09/2025

CONTENIDO

INTRODUCCIÓN

Investigadores de seguridad han descubierto un nuevo tipo de ataque Rowhammer, apodado Phoenix. Este ataque (identificado como CVE-2025-6202 con una puntuación CVSS de 7.1) es notable porque es capaz de burlar las protecciones avanzadas integradas en los chips de memoria DDR5, como el ECC (Código de Corrección de Errores) interno y el TRR (Target Row Refresh).

NUEVO ATAQUE LLAMADO PHOENIX ROWHAMMER ROMPE LA SEGURIDAD DE LA MEMORIA DDR5 EN SEGUNDOS

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2025_09_16_3
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	16/09/2025
Es día cero (0 day):	No

RESUMEN

Un equipo de investigadores ha descubierto un nuevo ataque llamado Phoenix (CVE-2025-6202), que es capaz de eludir las protecciones avanzadas integradas en los chips de memoria DDR5.

Detalles técnicos del ataque

El ataque Phoenix logra eludir las defensas de DDR5, como TRR (Target Row Refresh) y el ECC interno, que se consideraban robustas contra este tipo de ataques.

El ataque utiliza un patrón de activaciones específicas durante los intervalos de refresco de la memoria. Está diseñado para “golpear” filas de memoria solo en los momentos en que el TRR no las está revisando, aprovechando estos puntos ciegos para inducir los cambios de bit.

Además, el ataque tiene una característica novedosa de sincronización automática-correctiva. A diferencia de ataques anteriores que perdían eficacia si se desincronizaban con el proceso de refresco de la memoria, Phoenix se realinea automáticamente para seguir funcionando.

Ejemplo de explotación práctica

En tan solo 109 segundos, el exploit desarrollado por los investigadores pudo obtener privilegios de root en un sistema de escritorio configurado por defecto. En pruebas adicionales, demostraron que es posible:

- Modificar entradas de página para lograr la lectura y escritura de memoria arbitraria.
- Comprómetro claves RSA-2048 de máquinas virtuales para vulnerar autenticaciones SSH.
- Modificar el sudo binario para escalar privilegios de usuario a root.

Implicaciones y limitaciones

La principal implicación de este descubrimiento es que la vulnerabilidad está en el hardware de la memoria, no en el software. Esto significa que los módulos DDR5 ya fabricados y en uso no pueden ser parcheados.

Como medida de mitigación, los investigadores encontraron que aumentar la tasa de refresco de la memoria DRAM al triple (3× el valor estándar) detuvo el ataque Phoenix en los dispositivos probados. Sin embargo, esto tiene un costo de rendimiento y podría causar un aumento de calor o sobrecarga energética.

Es importante notar que, aunque todos los chips DDR5 de SK Hynix probados resultaron vulnerables, los resultados dependen de factores como el intervalo de refresco, la temperatura y el voltaje, lo que significa que la efectividad del ataque puede variar entre diferentes sistemas.

RECOMENDACIONES

- Aumente la tasa de refresco de la memoria: La mitigación más directa identificada por los investigadores es configurar la BIOS/firmware para aumentar la tasa de refresco de la memoria RAM.
- Implementa el principio del mínimo privilegio: El ataque busca la escalada de privilegios a nivel de raíz. Es crucial que los usuarios y las aplicaciones se ejecuten con los menores privilegios posibles para limitar el daño en caso de un compromiso inicial.
- Controla el acceso físico a los dispositivos: Dado que el ataque requiere acceso local, restringir el acceso físico a las computadoras es una clave de defensa.
- Mantén tus sistemas operativos y software actualizados: Aunque la vulnerabilidad es de hardware, los atacantes suelen explotar vulnerabilidades de software (por ejemplo, en el sistema operativo) para obtener el acceso local necesario para lanzar un ataque Rowhammer.

NOTICIA COMPLETA

https://devel.group/blog/un-nuevo-ataque-llamado-phoenix-rowhammer-rompe-la-seguridad-de-la-memoria-ddr5-en-segundos/

CONTACTOS DE SOPORTE

Correo electrónico: cti@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://devel.group