O novo ataque de Phoenix Rowhammer ignora as proteções de chips DDR

Data: 2025-09-16 09:23:11

Autor: Inteligência Against Invaders

Uma nova variação do ataque de Rowhammer, denominadaphoenix, rompe as defesas embutidas

dos modernos módulos de memória DDR5.

Pesquisadores Engenharia reversa As proteções no dram em chips SK Hynix e encontraram pontos cegos que os deixam girar, apesar das salvaguardas de hardware mais avançadas.

Seu trabalho mostra que todo módulo DDR5 testado da maior fabricante de DRAM do mundo permanece vulnerável a padrões de martelamento cuidadosamente projetados.

Descobrindo lacunas nas defesas DDR5

A SK Hynix adicionou atualização de linha de destino (TRR) para combater o Rowhammer por linhas refrescantes que veem uso pesado.

Os padrões anteriores não puderam enganar essas mitigações; portanto, a equipe de pesquisa usou testes baseados em FPGA para mapear quando e como ocorreu as atualizações do TRR.

Ao aumentar o comprimento de seus padrões de martelo, eles viram que a proteção se repete a cada 128 intervalos de atualização – oito vezes mais do que o assumido pelos ataques existentes.

___Iframe_placeholder_0___

Eles então perfuraram os primeiros e os últimos 64 intervalos. Na parte inicial, eles não encontraram amostragem consistente, enquanto a parte posterior mostrou refrescos pulando dois em cada quatro intervalos. Esses intervalos levemente amostrados se tornaram o ponto de entrada para novos padrões de ataque.

Usando suas descobertas, a equipe construiu dois padrões frescos de filmes de rowhammer. O padrão mais curto abrange 128 intervalos de atualização, evitando o primeiro segmento inconsistente e martelando apenas as janelas levemente amostradas.

A repetição deste segmento dezesseis vezes permite que ele entre milhares de intervalos sem desencadear defesas internas. O padrão mais longo cobre 2.608 intervalos e explora os mesmos pontos cegos com controle de tempo ainda mais fino.

Testado em quinze Dimms SK Hynix fabricados entre 2021 e 2024, o padrão curto teve sucesso em oito módulos, enquanto o longo trabalhava no resto.

Ambos os padrões podem desencadear milhares de bits – em média quase 5.000 por corrida – e

cada módulo era vulnerável a pelo menos um deles.

Um obstáculo crítico estava permanecendo em sincronia com o Dram Atualizar os comandos por períodos tão longos. Métodos atuais como o Zenhammer perdem o alinhamento muito rapidamente.

A Phoenix apresenta uma sincronização de auto-corrigir que rastreia a periodicidade da atualização e realinha o padrão sempre que uma atualização é perdida.

Isso garante martelamento confiável em milhares de intervalos. Com esse método, a equipe construiu a primeira exploração pública de escalada de privilégios de rowhammerge em uma configuração padrão de PC, alcançando o acesso total à raiz em apenas 109 segundos.

Os pesquisadores também demonstraram ataques a alvos do mundo real. Todo módulo DDR5 testado permitia a manipulação de entradas de página da mesa para ganhar memória arbitrária Leia/escreva.

A maioria dos DIMMs (73 %) expôs as teclas RSA-2048 em máquinas virtuais co-localizadas, arriscando quebras de SSH. Um terço dos módulos permitiu que os atacantes substituam o binário sudo a escalar privilégios locais.

Ao reproduzir a exploração do Rubicon Sudo no DDR5, eles mostraram tempos médios de exploração de pouco mais de cinco minutos.

Phoenix prova que mesmo as mais recentes defesas do DDR5 podem ser superadas com tempo preciso e design de padrões. As descobertas exigem novas estratégias de dram para interromper os futuros ataques de Rowhammer.

Encontre esta história interessante! Siga -nos LinkedIn**e**X**Para obter mais atualizações instantâneas**.