Faça root em menos de dois minutos: como a Phoenix explora vulnerabili

Data: 2025-09-20 13:34:03

Autor: Inteligência Against Invaders

Redazione RHC**:20 Setembro 2025 15:33**

Um**nova variante de ataques Rowhammer** foi desenvolvido para contornar os mecanismos de segurança mais recentes da SK Hynix **DDR5** batatas fritas. Apelidado Phoenix, o ataque permite acesso root a sistemas baseados em DDR5 em menos de dois minutos.

Lembre-se de que o original Martelo de remo ataque foi planejado por especialistas em **Universidade Carnegie Mellon** em 2014. Sua essência reside no fato de que *A manipulação intensa de algumas células de memória pode causar uma mudança no estado dos bits nas células adjacentes.*

As células de memória armazenam informações na forma de cargas elétricas, que determinam o valor dos bits dentro delas, ou seja, 1 ou 0. Devido ao aumento da densidade das células, *"golpes de martelo" repetidos (quando um aplicativo acessa as mesmas áreas milhares de vezes em uma fração de segundo) podem alterar o estado de carga em linhas adjacentes, causando "inversões de bits".*Daí o nome "Rowhammer".

Um dos mecanismos de defesa contra ataques de Rowhammer é chamado **Atualização de linha de destino (TRR).** Previne **inversão de bits** acionando atualizações de linha adicionais quando acessos frequentes a uma linha específica são detectados.

O **Martelo de remo Phoenix** ataque foi desenvolvido por **Google e a equipe COMSEC do Instituto Federal Suíço de Tecnologia em Zurique (ETH Zurique).** O relatório observa que o ataque foi testado em chips de memória DDR5 da Hynix (um dos maiores fabricantes de chips de memória, com uma participação de mercado de aproximadamente 36%), mas a Phoenix também pode ameaçar produtos de outros fabricantes.

Depois de analisar as defesas sofisticadas implementadas pela Hynix para proteger contra ataques Rowhammer e examinar sua operação, os pesquisadores descobriram que alguns intervalos de atualização não eram monitorados por defesas, o que poderia ter sido explorado por um invasor hipotético.

Os especialistas também desenvolveram um método que permite ao Phoenix rastrear e sincronizar milhares de operações de atualização, realizando autocorreção quando as ausentes são detectadas. Para ignorar a proteção TRR, o Phoenix abrange intervalos de atualização de 128 e 2608 e atua apenas em slots de ativação específicos em momentos específicos.

Como resultado, os pesquisadores foram capazes de "inverter" os bits em todos os 15 chips de

memória DDR5 no pool de testes e criar uma exploração de escalonamento de privilégios usando o Rowhammer. Os testes mostraram que *obter um shell raiz "em um sistema DDR5 típico com configurações padrão" levou apenas 109 segundos.*

Os autores de Phoenix também exploraram a potencial aplicação prática desse ataque para obter o controle de um sistema de alvo. Eles descobriram que, ao direcionar PTEs para criar primitivas de leitura/gravação arbitrárias, todos os produtos testados tinham a vulnerabilidade. Em outro teste, os pesquisadores visaram as chaves RSA-2048 da máquina virtual para quebrar a autenticação SSH e descobriram que 73% dos DIMMs eram vulneráveis a esse ataque.

Em um terceiro experimento, os pesquisadores descobriram que poderiam modificar o binário sudo para elevar os privilégios locais para root em 33% dos chips testados. Como mostra a tabela, todos os chips de memória testados eram vulneráveis a pelo menos um dos padrões Rowhammer do ataque Phoenix. O padrão mais curto, com intervalos de atualização de 128, mostrou-se mais eficaz e gerou mais flips em média.

A questão Phoenix recebeu o identificador CVE-2025-6202, e os invasores alertam que isso afeta todos os **DIMMs de RAM fabricados entre janeiro de 2021 e dezembro de 2024.**

Embora o Rowhammer seja um problema de segurança em todo o setor e **não pode ser corrigido nos módulos de memória atualmente enviados, os usuários podem se proteger do Phoenix triplicando o intervalo de atualização da DRAM (tREFI).** No entanto, observou-se que isso pode causar erros e corrupção de dados, resultando em instabilidade geral do sistema.

Além de um relatório detalhado sobre o novo ataque, os pesquisadores publicaram tudo o que é necessário para reproduzir Phoenix no GitHub. O repositório inclui experimentos FPGA para reverter implementações de TRR e código de exploração de prova de conceito.

Redação
A equipe editorial da Red Hot Cyber é composta por um grupo de indivíduos e fontes anônimas que colaboram ativamente para fornecer informações e notícias antecipadas sobre segurança cibernética e computação em geral.

Lista degli articoli