A Apple apresenta a Imposição de Integridade de Memória. Será este o fim

Data: 2025-09-15 05:28:03

Autor: Inteligência Against Invaders

Redazione RHC**:15 Setembro 2025 07:26**

A Apple apresentou oficialmente **Imposição de integridade de memória,** um novo sistema de proteção de memória que a empresa chama de *o avanço mais significativo já feito na segurança do sistema operacional do consumidor.* Demorou cinco anos para desenvolver e combinar os recursos de hardware do Apple Silicon com os recursos de software do iOS e macOS.

De acordo com os engenheiros, **Os usuários do iPhone 17 e iPhone Air agora têm a primeira proteção de memória sempre ativa do setor,** que funciona sem nenhum impacto significativo no desempenho. A empresa enfatiza que, *até agora, nenhum malware de mercado de massa conseguiu penetrar nas defesas do iOS*. Os únicos ataques sistêmicos registrados vêm do arsenal de *spyware comercial usado por agências governamentais e custando milhões de dólares.*

O elemento comum de todas essas cadeias de hackers é **vulnerabilidades de gerenciamento de memória.**Eles continuam sendo o principal alvo dos invasores, e a Imposição de Integridade de Memória foi projetada para bloquear esse vetor de ataque.

O novo mecanismo é baseado em várias camadas. O primeiro passo foi implementar alocadores de memória seguros: *kalloc_type para o kernel, xzone malloc* no *Espaço do usuário* nível, e *libpas no WebKit.* Esses alocadores usam informações de tipo para organizar blocos de memória para que os invasores não possam sobrepor objetos diferentes. **Isso torna impossíveis ataques como Buffer Overflow e Use-After-Free.**

No entanto, os alocadores por si só não são suficientes: eles trabalham com grandes blocos de 16 KB e nem sempre protegem contra ataques dentro de um único tipo. Para atingir esse objetivo, a Apple, juntamente com a Arm, reformulou o **Extensão de marcação de memória** especificação e implementou uma versão melhorada: **MTE aprimorado.** Agora, cada área de memória é marcada com uma tag secreta e o acesso só é possível se houver uma correspondência. Qualquer tentativa de acessar além do buffer alocado ou de usar uma área já liberada **é bloqueado no nível do processador e o sistema encerra o processo.**

Para fortalecer a proteção, a Apple introduziu o **Aplicação de confidencialidade de tags** mecanismo. Ele evita o vazamento de dados por meio de canais de terceiros e também protege contra ataques que usam execução especulativa. Especificamente, os engenheiros eliminaram três cenários em que os dados de serviço poderiam ser extraídos por meio de diferenças nos tempos de processamento de instruções ou vulnerabilidades, como **Espectro V1. O iPhone 17 apresenta uma otimização exclusiva: o kernel limita os deslocamentos de ponteiro usando um padrão de 0x2BAD especial, praticamente eliminando a possibilidade de ataques confiáveis com**

saturações arbitrárias de memória.

Um passo importante foi a operação síncrona e contínua de **MIE**. Ao contrário do clássico **MTE**, onde os desenvolvedores podem habilitar o tratamento de erros diferido, a Apple essencialmente abandonou esse modelo, pois deixa uma janela para ataques. O suporte de hardware é fornecido pelo novo **A19 e A19 Pro** chips, que alocam recursos adicionais para armazenar tags e realizar verificações.

Foi dada especial atenção às aplicações de terceiros. A proteção se estende não apenas aos processos do sistema e ao kernel, mas também aos programas pelos quais usuários específicos são atacados com mais frequência: mensagens instantâneas, redes sociais e clientes de e-mail. Os desenvolvedores já podem testar o EMTE no Xcode como parte do pacote de segurança aprimorada.

A equipe vermelha da Apple passou cinco anos tentando contornar o MIE simulando cadeias de exploração antigas e novas. A conclusão foi clara: **as velhas técnicas não funcionam mais**. A maioria das vulnerabilidades se torna inutilizável e as restantes raramente permitem a criação de um exploit totalmente funcional. Mesmo que eles detectem um bug com sucesso, o resto da cadeia entra em colapso e os invasores devem começar de novo.

A Apple diz que *A aplicação da integridade da memória aumenta drasticamente o custo e a complexidade da criação de spyware comercial.* As auditorias internas mostraram que muitas técnicas usadas nos últimos 25 anos não são mais aplicáveis. A empresa chama essa tecnologia de o avanço mais significativo na proteção de memória na história dos sistemas operacionais de consumo.

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

Lista degli articoli