O Google Project Zero divulga a vulnerabilidade da Apple, permitindo o de

Data: 2025-09-29 05:01:50

Autor: Inteligência Against Invaders

O pesquisador do Google Project Zero Jann Horn divulgou uma nova vulnerabilidade nos sistemas MacOS e iOS da Apple, que poderiam permitir que os invasores ignorem as proteções de randomização do layout do espaço de endereço (ASLR) através de vazamentos de ponteiro nos processos de serialização.

Visão geral da vulnerabilidade

A vulnerabilidade explora uma técnica que aproveita as estruturas de dados com chave de ponteiro na estrutura de serialização do NSkeyedarchiver da Apple para vazar endereços de memória sem exigir violações de segurança da memória ou ataques de tempo.

O ataque funciona quando um aplicativo merece dados fornecidos pelo atacante, re-serializa os objetos resultantes e retorna os dados serializados ao invasor.

O pesquisador descoberto Esse problema durante o projeto interno Zero Zero Discussões sobre vazamentos remotos de ASLR que seriam necessários para explorar certos bugs de corrupção de memória nos dispositivos Apple.

Embora nenhuma superfície de ataque do mundo real específica tenha sido identificada em macos Ou iOS, Horn demonstrou com sucesso a técnica usando a serialização do NSkeyedarchiver em um caso de teste artificial.

Detalhes técnicos

O ataque explora vários componentes -chave da estrutura principal da Apple Foundation:

Exploração NSNULL Singleton: A vulnerabilidade aproveita a instância do CFNULL Singleton armazenada no cache compartilhado, que usa endereços de ponteiro como códigos de hash quando nenhum manipulador de hash personalizado é fornecido.

Manipulação da tabela de hash de nsdictionary: Os invasores podem manipular as tabelas de hash do nsdictionary inserindo as teclas NSNumber cuidadosamente escolhidas que mapeiam para baldes de hash específicos, criando padrões previsíveis na estrutura de dados.

Análise de ordem de serialização: Ao analisar a ordem das chaves em objetos reerializados do nsdictionary, os atacantes podem determinar Hash Bucket Locais e extrair informações sobre endereços de memória.

A técnica envolve o envio de aproximadamente 50kb de dados serializados especialmente criados, contendo várias instâncias nsdicionárias com padrões específicos de teclas NSNumber e nsnull.

Quando o aplicativo de destino se desapealiza e serializa esses dados, a ordem dos elementos na saída revela informações sobre o endereço de memória do NSNULL Singleton.

Embora essa vulnerabilidade represente um ataque teórico sem impacto no mundo real demonstrado, ela mostra como o hash baseado em ponteiro nas estruturas de dados com chave pode levar a vazamentos de abordar sob condições específicas.

A técnica pode ser potencialmente combinada com outras façanhas para derrotar as proteções do ASLR, tornando os ataques de corrupção da memória mais confiáveis.

A pesquisa baseia -se em trabalhos anteriores em ataques de colisão de hash e demonstra novas abordagens à divulgação de informações por meio de mecanismos de serialização.

A Apple abordou essa vulnerabilidade em seus lançamentos de segurança de 31 de março de 2025. A mitigação mais robusta envolve evitar endereços de objetos como teclas de pesquisa ou implementar funções de hash com chave para reduzir possíveis vazamentos de endereço para apontar os oráculos da igualdade.

O Projeto Zero relatou esse problema diretamente à Apple sem arquivá-lo em seu rastreador público de bugs devido à falta de superfícies de ataque do mundo real demonstradas.

A divulgação destaca a importância das práticas seguras de serialização e as possíveis implicações de segurança dos mecanismos de hash baseados em ponteiros nas estruturas do sistema.