Apple pede aos usuários que atualizem o iPhone e o Mac para corrigir o bu

Data: 2025-10-01 11:02:11

Autor: Inteligência Against Invaders

Apple pede aos usuários que atualizem o iPhone e o Mac para corrigir o bug da fonte

A Apple lançou atualizações do iOS e do macOS para corrigir uma falha no processamento de fontes que poderia desencadear uma condição de negação de serviço ou corrupção de memória.

A Apple lançou atualizações do iOS e do macOS para resolver uma falha de gravidade média, rastreada como CVE-2025-43400, no processamento de fontes que pode desencadear uma condição de negação de serviço ou corrupção de memória.

A falha CVE-2025-43400 é um problema de gravação fora dos limites no componente FontParser do sistema operacional. Uma vulnerabilidade de gravação fora dos limites (OOB) ocorre quando um programa grava dados fora do buffer de memória alocado para ele. Isso pode corromper a memória adjacente, levando a travamentos, comportamento imprevisível ou até mesmo permitindo que invasores executem código arbitrário.

Um invasor pode criar uma fonte maliciosa que pode fazer com que os aplicativos falhem ou corrompam a memória do processo, potencialmente levando à execução de código arbitrário.

“O processamento de uma fonte criada com códigos maliciosos pode levar ao encerramento inesperado do aplicativo ou à corrupção da memória do processo.” lê o comunicado*. “Um problema de gravação fora dos limites foi resolvido com a verificação aprimorada dos limites.”*

A Apple emitiu atualizações para iOS 26, macOS 26e plataformas mais antigas para resolver o bug. As versões incluem iOS/iPadOS 26.0.1, 18.7.1, macOS 26.0.1, 15.7.1, 14.8.1 e visionOS 26.0.1.

“Normalmente, as fontes são arquivos seguros e padronizados usados diariamente em inúmeros aplicativos e sites, mas devido a essa vulnerabilidade, um invasor pode criar um arquivo de fonte especialmente criado contendo dados manipulados que exploram vulnerabilidades no mecanismo de processamento de fontes do sistema operacional. Quando essa fonte maliciosa é carregada por um aplicativo ou processo do sistema, ela pode causar corrupção ou falhas na memória. Na pior das hipóteses, isso pode permitir que os invasores executem códigos prejudiciais remotamente, ganhando controle sobre o dispositivo.” lê o análise *publicado pela Malwarebytes. “Dado que as fontes são amplamente utilizadas e muitas vezes processadas silenciosamente em segundo plano, as vulnerabilidades de fontes representam um vetor de risco significativo para invasores que pretendem comprometer dispositivos.”*

CERT de Hong Kong Consultivo confirma que um invasor remoto pode explorar a vulnerabilidade

remotamente.

As atualizações estão disponíveis para iPhone 11 e posterior, iPad Pro de 12,9 polegadas de 3ª geração e posterior, iPad Pro de 11 polegadas de 1ª geração e posterior, iPad Air de 3ª geração e posterior, iPad de 8ª geração e posterior e iPad mini de 5ª geração e posterior

No momento, não está claro se a falha foi explorada em ataques na natureza. Os usuários devem atualizar seus dispositivos o mais rápido possível.

Siga-me no Twitter:@securityaffairseLinkedineMastodonte

PierluigiPaganini

(Assuntos de Segurança–hacking,iOS)