Vulnerabilidade do dia zero do WhatsApp explorado com ataques de 0 cliq

Data: 2025-08-29 19:14:31

Autor: Inteligência Against Invaders

O WhatsApp emitiu um aviso crítico de segurança abordando uma vulnerabilidade de dias zero

recém-descoberta, rastreada como CVE-2025-55177, que foi explorada em ataques de clique zero

altamente sofisticados direcionados aos usuários de Mac e iOS.

A vulnerabilidade, combinada com uma falha no nível do sistema operacional (CVE-2025-43300), gerou alarmes sobre o potencial comprometimento dos dispositivos e dados do usuário, incluindo mensagens confidenciais.

Detalhes da vulnerabilidade

A vulnerabilidade descoberto pela investigação do WhatsApp, detalhado em uma sexta -feira Consultor de segurançarevelou que a falha ocorre de uma “autorização incompleta de mensagens de sincronização de dispositivos vinculados” no WhatsApp para iOS (antes da versão 2.25.21.73), o WhatsApp Business for iOS (antes da v2.25.21.78) e o WhatsApp para Mac (antes da v2.25.25.78).

Essa vulnerabilidade permitiu que um usuário não relacionado acionasse o processamento do conteúdo de uma URL arbitrária no dispositivo de um destino, ignorando a necessidade de qualquer interação do usuário-daí a designação de “clique zero”.

A gravidade aumentou quando foi descoberto que essa falha do WhatsApp foi explorada em conjunto com CVE-2025-43300uma vulnerabilidade fora dos limites escreve na estrutura Imageio da Apple.

A Apple já havia corrigido esse problema no nível do sistema operacional, confirmando sua exploração em “ataques extremamente sofisticados contra indivíduos direcionados específicos”.

A combinação dessas vulnerabilidades criou um potente vetor de ataque, levando potencialmente à corrupção da memória e acesso não autorizado aos dados do dispositivo.

Investigação em andamento

O incidente provocou uma investigação ativa do Laboratório de Segurança da Anistia Internacional, que está examinando casos envolvendo vários indivíduos direcionados nesta campanha.

Indicações iniciais sugerem que o Ataque do WhatsApp está impactando os usuários do iPhone e do Android, com indivíduos da sociedade civil, incluindo jornalistas e defensores de direitos humanos, entre os afetados.

? Quebra: Novo Exploração Zero Click usado para invadir usuários do WhatsApp.

O WhatsApp acabou de enviar uma rodada de notificações de ameaça para os indivíduos que eles acreditam onde direcionados por uma campanha avançada de spyware nos últimos 90 dias.

Procure ajuda especializada se você recebeu este alerta pic.twitter.com/i4chlsinor

– Donncha Ó Cearbhaill (@Donnchac) 29 de agosto de 2025

A ameaça persistente de spyware do governo continua a pôr em risco esses grupos, ressaltando a necessidade de medidas de proteção robustas.

Notavelmente, a vulnerabilidade da Apple (CVE-2025-43300) reside em uma biblioteca de imagens principais, o que significa que poderia ser explorado por outros aplicativos além do WhatsApp.

“CVE-2025-55177, um desvio de autorização no WhatsApp no ??iOS e Mac, permitiu que os atacantes forcem“ o conteúdo de um URL arbitrário ”a ser renderizado no dispositivo de um alvo”.

O WhatsApp e os especialistas em segurança aconselham as etapas a seguir para mitigar os riscos:

- Atualize o WhatsApp para a versão mais recente (iOS v2.25.21.73 ou posterior, IOS V2.25.21.78 ou posterior, Mac v2.25.21.78 ou posterior).
- Instale as atualizações mais recentes do sistema operacional para iOS, iPados e macOS.
- Ative recursos de segurança aprimorados, como o modo de bloqueio no iOS ou proteção avançada no Android.

Encontre esta notícia interessante! Siga -nos Google News**Assim,**LinkedIn**e**X**Para obter atualizações instantâneas!**