BOLETIM DE SEGURANÇA

Apple corrige vulnerabilidade de Bluetooth dos AirPods que pode permitir espionagem

heimdall
security research
A DIVISION OF ISH

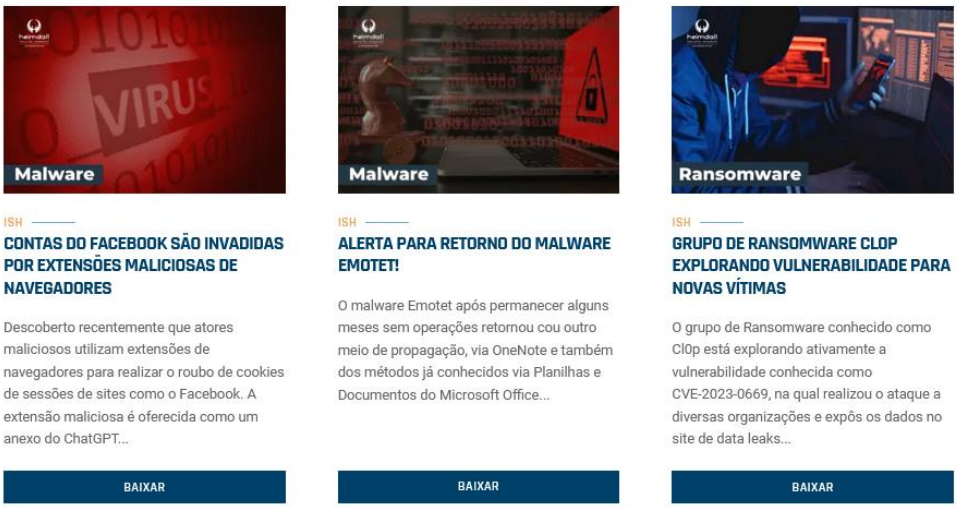
TLP: CLEAR

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso **X**.

Heimdall Security Research

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

Boletins de Segurança – Heimdall



SUMÁRIO

1 SUMÁRIO EXECUTIVO

A Apple lançou uma atualização de firmware para AirPods que pode permitir que um invasor obtenha acesso aos fones de ouvido de maneira não autorizada.

2 INFORMAÇÕES SOBRE A VULNERABLIDADE

A vulnerabilidade CVE-2024-27867 descoberta pelo pesquisador Jonas Dreßler, refere-se a um problema de autenticação que afeta **AirPods** (2ª geração e posteriores), **AirPods Pro** (todos os modelos), **AirPods Max**, **Powerbeats Pro** e **Beats Fit Pro**. Quando seus fones de ouvido estão buscando uma solicitação de conexão para um de seus dispositivos emparelhados anteriormente, um invasor no alcance do Bluetooth pode falsificar o dispositivo de origem pretendido e obter acesso aos seus fones de ouvido. Em outras palavras, um adversário fisicamente próximo poderia explorar a vulnerabilidade para escutar conversas privadas. A Apple disse que o problema foi resolvido com uma melhor gestão do estado.

Ela foi corrigida como parte da atualização de firmware dos AirPods 6A326, atualização de firmware dos AirPods 6F8 e atualização de firmware do Beats 6F8. O desenvolvimento ocorre duas semanas depois que o fabricante do iPhone lançou atualizações para o visionOS (versão 1.2) para corrigir 21 deficiências, incluindo sete falhas no mecanismo do navegador WebKit.

Um dos problemas diz respeito a uma falha lógica (CVE-2024-27812) que pode resultar em negação de serviço (DoS) ao processar conteúdo da web. O problema foi corrigido com um melhor manuseio de arquivos. O pesquisador de segurança Ryan Pickren, que relatou a vulnerabilidade, descreveu-a como o "primeiro hack de computação espacial do mundo" que poderia ser transformado em arma para "ignorar todos os avisos e preencher sua sala à força com um número arbitrário de objetos 3D animados" sem interação do usuário.

A vulnerabilidade aproveita a falha da Apple em aplicar o modelo de permissões ao usar o recurso ARKit Quick Look para gerar objetos 3D no quarto da vítima. Para piorar a situação, esses objetos animados continuam a persistir mesmo depois de sair do Safari, pois são manipulados por um aplicativo separado.

3 RECOMENDAÇÕES

É necessário realizar atualização conforme recomendações do fabricante. As atualizações de firmware são feitas automaticamente enquanto os AirPods estão carregando e no alcance do Bluetooth do iPhone, iPad ou Mac conectados ao Wi-Fi. Você também pode usar o iPhone, iPad ou Mac para verificar se os AirPods estão com a versão mais recente.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- Apple
- Theahckernews
- NVD

5 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH