TLP: CLEAR

BOLETIM DE SEGURANÇA

Apple lança patches para corrigir falhas em iPhones, Macs e outros dispositivos

heimdall
security research

Acesse a nossa nova comunidade através do WhatsApp!

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 INTRODUÇÃO EXECUTIVA

A Apple lançou atualizações de segurança para corrigir a vulnerabilidade CVE-2025-24085, que afeta diversos dispositivos, incluindo iPhones, Macs, Apple TVs, Apple Vision Pro e Apple Watches. Esta falha, já explorada ativamente, permite que aplicativos maliciosos elevem seus privilégios no sistema.

2 INFORMAÇÕES SOBRE A VULNERABILIDADE

A CVE-2025-24085 é uma vulnerabilidade do tipo "*use-after-free*" no componente Core Media dos sistemas operacionais da Apple. Essa falha ocorre quando a memória é indevidamente acessada após ter sido liberada, permitindo que um aplicativo malicioso já instalado no dispositivo execute operações com privilégios elevados. A exploração bem-sucedida dessa vulnerabilidade pode comprometer a integridade e a segurança do sistema afetado.

2.1 SISTEMAS E PRODUTOS AFETADOS

Os seguintes sistemas e dispositivos são afetados pela vulnerabilidade:

iOS 18.2.1 e iPadOS 18.2.1

- iPhone XS e modelos posteriores
- iPad Pro de 13 polegadas
- iPad Pro de 12,9 polegadas (3ª geração e posteriores)
- iPad Pro de 11 polegadas (1ª geração e posteriores)
- iPad Air (3ª geração e posteriores)
- iPad (7ª geração e posteriores)
- iPad mini (5ª geração e posteriores)

macOS Sequoia 15.2

- Macs executando o macOS Sequoia

tvOS 18.2.1

- Apple TV HD e Apple TV 4K (todos os modelos)

visionOS 2.2

- Apple Vision Pro

watchOS 11.2

- Apple Watch Series 6 e modelos posteriores

2.2 IMPACTO DA VULNERABILIDADE

Os principais impactos da vulnerabilidade CVE-2025-24085 são:

- Elevação de privilégios
- Comprometimento da integridade do sistema
- Acesso não autorizado a dados sensíveis
- Instalação de software malicioso
- Perda de privacidade
- Impacto na disponibilidade do sistema

3 RECOMENDAÇÕES

É essencial que os usuários dos dispositivos afetados instalem as atualizações de segurança disponibilizadas pela Apple com a máxima urgência. As versões corrigidas dos sistemas operacionais já estão disponíveis e incluem:

- **iOS e iPadOS**: Atualizar para a versão *18.3*.
- **macOS Sequoia**: Atualizar para a versão *15.3*.
- **tvOS**: Atualizar para a versão *18.3*.
- **visionOS**: Atualizar para a versão *2.3*.
- **watchOS**: Atualizar para a versão *11.3*.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Apple**
- **CVE**
- **The Hacker News**

5 AUTORES

- **Rafael Salomé**

heimdall
security research
A DIVISION OF ISH