



BOLETIM DE SEGURANÇA

Vulnerabilidades de *zero-day* da
Apple recebe correções



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](#)



ISH

CONTAS DO FACEBOOK SÃO INVADIDAS POR EXTENSÕES MALICIOSAS DE NAVEGADORES

Descoberto recentemente que atores maliciosos utilizam extensões de navegadores para realizar o roubo de cookies de sessões de sites como o Facebook. A extensão maliciosa é oferecida como um anexo do ChatGPT...

BAIXAR



ISH

ALERTA PARA RETORNO DO MALWARE EMOTET!

O malware Emotet após permanecer alguns meses sem operações retornou cou outro meio de propagação, via OneNote e também dos métodos já conhecidos via Planilhas e Documentos do Microsoft Office...

BAIXAR



ISH

GRUPO DE RANSOMWARE CLOP EXPLORANDO VULNERABILIDADE PARA NOVAS VÍTIMAS

O grupo de Ransomware conhecido como CLOP está explorando ativamente a vulnerabilidade conhecida como CVE-2023-0669, na qual realizou o ataque a diversas organizações e expôs os dados no site de data leaks...

BAIXAR

SUMÁRIO

1	Vulnerabilidades corrigidas - Apple	4
2	Referências	5

1 VULNERABILIDADES CORRIGIDAS - APPLE

A **Apple** publicou atualizações de segurança para solucionar algumas falhas de segurança, incluindo **duas vulnerabilidades** que foram exploradas ativamente.

As vulnerabilidades são:

- **CVE-2024-23225:** Um problema de corrupção de memória no Kernel que um invasor com capacidade arbitrária de leitura e gravação do kernel pode explorar para contornar as proteções de memória do kernel.
Base de Pontuação: (ainda não divulgado)
- **CVE-2024-23296:** Um problema de corrupção de memória no sistema operacional em tempo real (RTOS) RTKit que um invasor com capacidade arbitrária de leitura e gravação de kernel pode explorar para ignorar as proteções de memória do kernel.
Base de Pontuação: (ainda não divulgado)

Ainda não é possível determinar como as vulnerabilidades estão sendo exploradas, mas que de acordo com a Apple, **ambas as vulnerabilidades foram resolvidas com validação aprimorada no iOS 17.4, iPadOS 17.4, iOS 16.7.6 e iPadOS 16.7.6.**

As **atualizações** estão disponíveis para os dispositivos:

- **iOS 16.7.6 e iPadOS 16.7.6:** iPhone 8, iPhone 8 Plus, iPhone X, iPad 5ª geração, iPad Pro de 9,7 polegadas e iPad Pro de 12,9 polegadas de 1ª geração.
- **iOS 17.4 e iPadOS 17.4:** iPhone XS e posterior, iPad Pro de 12,9 polegadas de 2ª geração e posterior, iPad Pro de 10,5 polegadas, iPad Pro de 11 polegadas de 1ª geração e posterior, iPad Air de 3ª geração e posterior, iPad de 6ª geração e posterior e iPad mini de 5ª geração e posterior.

Com o patch mais recente, a Apple resolveu um total de três zero-day explorados ativamente em seu software desde o início do ano. Lembrando que ao final de janeiro de 2024, a Apple corrigiu uma falha de confusão de tipo no WebKit (**CVE-2024-23222**) afetando iOS, iPadOS, macOS, tvOS e navegador Safari, a qual poderia resultar na execução remota de código.

2 REFERÊNCIAS

- **Heimdall by ISH Tecnologia**
- [iOS 16.7.6 e iPadOS 16.7.6](#)
- [iOS 17.4 e iPadOS 17.4](#)
- **CVE-2024-23225 - [NIST](#)**
- **CVE-2024-23296 - [NIST](#)**



heimdall
security research

A DIVISION OF ISH