ALERTA DE VULNERABILIDADE

Apple lança atualizações de segurança emergencial para correção de zero days exploradas em ataques

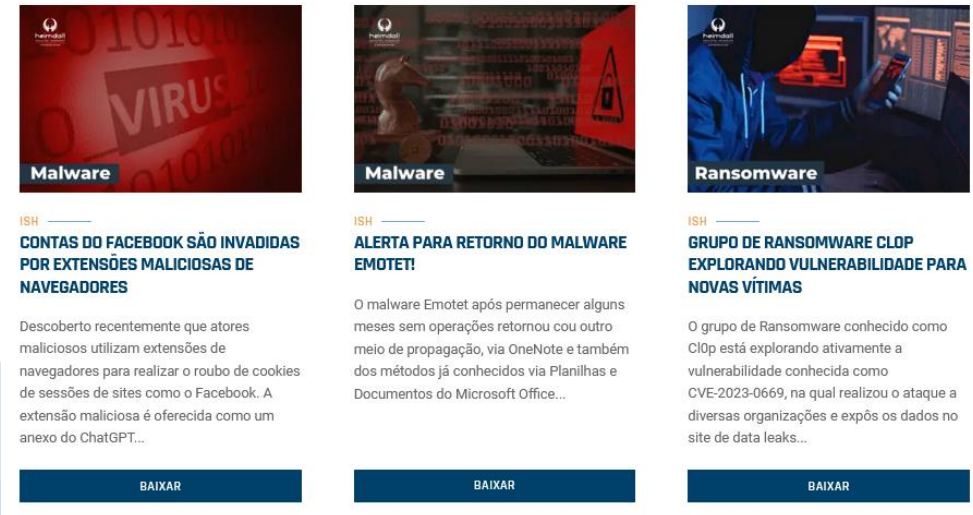
heimdall
security research
A DIVISION OF ISH

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

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



heimdall
security research

Sumário

1 INTRODUÇÃO

Nos últimos anos, as explorações cibernéticas em softwares da Apple têm se tornado uma preocupação crescente à medida que os dispositivos e sistemas operacionais da empresa ganham cada vez mais popularidade.

Neste contexto, explorar vulnerabilidades nos softwares da Apple se tornou uma meta atraente para atores de ameaças cibernéticas e pesquisadores de segurança. Essas explorações podem assumir diversas formas, desde vulnerabilidades que permitem o acesso não autorizado, monitoramento a dispositivos Apple até técnicas de engenharia social que visam enganar os usuários para que revelem informações confidenciais.

2 ATUALIZAÇÕES EMERGENCIAL DE SEGURANÇA

Recentemente a Apple lançou atualizações de segurança de emergência para corrigir três novas vulnerabilidades de dia zero exploradas em ataques direcionados a usuários de iPhone e Mac. Conforme é de costume, a Apple detém as informações detalhadas sobre as vulnerabilidades do iOS e as explorações que as aproveitam em sigilo.

Essa abordagem não é inesperada, pois a Apple retém esses detalhes até que o máximo de usuários possível tenha tido a chance de atualizar seus dispositivos. Isso é feito para evitar que outros invasores tirem vantagem das vulnerabilidades antes que os usuários tenham a oportunidade de se protegerem por meio das atualizações de segurança.

As vulnerabilidades corrigidas foram as seguintes:

- **CVE-2023-41992** - Vulnerabilidade no framework Kernel , permite que um invasor local eleve privilégios.
- **CVE-2023-41991** – Vulnerabilidade na estrutura de segurança, pode ser explorado por um aplicativo malicioso para ignorar a validação de assinatura.
- **CVE-2023-41993** – Vulnerabilidade no mecanismo do navegador WebKit, pode ser acionado pelo processamento de conteúdo da Web especialmente criado e pode levar à execução arbitrária de código.

3 DISPOSITIVOS E SISTEMAS

As atualizações estão disponíveis para os seguintes dispositivos e sistemas operacionais:

- **iOS 16.7** e **iPadOS 16.7** – iPhone 8 e posterior, iPad Pro (todos os modelos), iPad Air de 3ª geração e posterior, iPad de 5ª geração e posterior e iPad mini de 5ª geração e posterior
- **iOS 17.0.1** e **iPadOS 17.0.1** – 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 geração e posteriores, iPad mini 5ª geração e posteriores
- **macOS Monterey 12.7** e **macOS Ventura 13.6**
- **watchOS 9.6.3** e **watchOS 10.0.1** – Apple Watch Series 4 e posterior
- **Safari 16.6.1** - macOS Big Sur e macOS Monterey

4 Conclusão

A importância da atualização de segurança em dispositivos Apple e a existência de explorações por atores maliciosos é clara: a atualização de segurança é uma medida essencial para proteger dispositivos e dados em um cenário de ameaças crescentes. Os dispositivos da Apple, conhecidos por sua reputação de segurança, também são alvos de interesse para atores maliciosos que buscam explorar vulnerabilidades.

A atualização de patchs segurança é a principal defesa contra explorações cibernéticas, uma vez que corrige vulnerabilidades conhecidas e fortalece as defesas contra ameaças emergentes. Ignorar atualizações de segurança pode deixar dispositivos e dados vulneráveis a ataques, comprometendo a privacidade e a segurança dos usuários.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- thehackernews
- bleepingcomputer


heimdall
security research
A DIVISION OF ISH