Apple MacOS tem porta aberta para hackers black hat; empresa deve corrigir[1]

O ano mal começou e está difícil para a Apple. Enquanto a companhia está envolvida na questão "diminuição do desempenho x autonomia de bateria" sobre iPhones, um pesquisador de segurança publicou no primeiro dia de 2018 uma vulnerabilidade que atinge o sistema operacional MacOS desde 2002. Ou seja: uma porta aberta para hackers em computadores da Apple.

"Um pequeno e feio bug. Quinze anos. Sistema completamente comprometido", escreveu o pesquisador Siguza (S1guza) no Twitter. A prova foi publicada no Github.

Segundo Siguza, agentes maliciosos podem utilizar a vulnerabilidade de dia zero para conseguir controle total do computador.

Sobre a vulnerabilidade em si, estamos vendo uma falha de escalonamento de privilégios (LPE), ou seja, uma falha que permite aos hackers black hat o acesso root ao sistema, permitindo a execução de códigos maliciosos. A falha afeta a extensão kernel IOHIDFamily, desenvolvida para HID (dispositivo de interface humana) — um nome bonito para exemplificar touchscreens e botões.

Com o acesso root, os cibercriminosos conseguem desativar programas de segurança da Apple presentes na máquina, como Systema Integrity Protection e o Apple Mobile File Integrity. Escalonamento: ao desativar esses programas, novas portas são abertas.

Ao Threatpost, o pesquisador de vulnerabilidades Jasiel Spelman, da Zero Day Iniative, comentou o seguinte sobre o caso: "um atacante já precisa ter uma presença no sistema para tirar vantagem dessa vulnerabilidade. Isso pode ser feito ao infectar o sistema por meio de uma vulnerabilidade remota, como um bug do Safari, ou até via acesso físico, como um sistema kiosk. O maior problema dessa vulnerabilidade é que ela existe há anos. Pior ainda, essa vulnerabilidade possui existe em um componente open-source (código aberto)".

A Apple não entregou um posicionamento sobre o caso. É esperado que um patch de segurança chegue nas próximas semanas

"Meu objetivo primário era publicar para as pessoas lerem. Eu não venderia para black hats porque eu não quero ajudar essa 'causa'. Eu teria enviado para a Apple se o bug bounty deles incluísse o macOS, ou se a vulnerabilidade fosse explorada remotamente", finalizou Siguza.

- `poc ( make poc )`
  Targets all macOS versions, crashes the kernel to prove the existence of a memory corruption.
- `leak ( make leak )`
  Targets High Sierra, just to prove that no separate KASLR leak is needed.
- `hid ( make hid )`
  Targets Sierra and High Sierra (up to 10.13.1, see README), achieves full kernel r/w and disables SIP to prove that the vulnerability can be exploited by any unprivileged user on all recent versions of macOS.

[1] By Rogerinho Freitas| Janeiro 4th, 2018|Categories: Apple Inc., Hacking - *Fonte: THREATPOST*