Mac sticks with serious security holes

According to Ars Technica, security expert Pedro Vilaca found a Mac OS X vulnerability that allowed hackers to take over the Mac after exiting sleep. This vulnerability will affect all Macs released before mid-2014

A newly discovered security vulnerability could help hackers insert malicious code over the user's BIOS, causing the Mac to face the risk of permanent re-opening.

Detecting security holes on 1,500 iOS applications

According to Ars Technica, security expert Pedro Vilaca found a Mac OS X vulnerability that allowed hackers to take over the Mac after exiting sleep. This vulnerability will affect all Macs released before mid-2014.

At the moment, hackers cannot take advantage of this vulnerability to conduct a wide-ranging attack, but Vilaca's research shows that criminals can take advantage of this flaw to launch attacks on some individuals. determined.

In his study, Vilaca was able to flash the Mac's BIOS after the device exited sleep mode. Usually, this is impossible, but a flaw Apple missed will allow hackers to flash the BIOS. Malicious codes written on the BIOS will exist even if the user has formatted the hard drive or reinstalled the operating system.

Victims of similar attacks will not be able to recognize any signs when malicious code is being installed on the Mac's BIOS.

A very serious vulnerability will allow hackers to write malicious code over the user's BIOS, causing their Macs to face the risk of permanent backlog.

More dangerous, hackers do not need to be in direct contact with the Mac to achieve this type of attack. Instead, they can trick victims into visiting a website and then install hidden malicious code:

" *The only condition is that you ask the machine to go back to sleep mode. I have not studied this yet but you will be able to order the victim's machine to automatically switch back to sleep mode and activate this attack. remote* ", Vilaca confirmed with Ars Technica.

Once attacked, users will be faced with the risk of permanently re-opening the door on their Mac. The only way to find a victim is to use software that reads the BIOS chip data and compares it with the original firmware to find out if their BIOS has been changed.