The researcher released code that exploits the iOS Kernel vulnerability

Adam Donenfeld, a researcher at mobile security company Zimperium, has released the POC code for zIVA - a kernal vulnerability affecting iOS 10.3.1 and earlier.

Adam Donenfeld, a researcher at mobile security company Zimperium, has released the POC code for zIVA - a kernal vulnerability affecting iOS 10.3.1 and earlier.

The zIVA exploit code allows the RW (Read Write) attacker to randomly and root the device.

Apple has patched since May

Apple has handled eight critical weaknesses of this vulnerability in the security patch package released in May. One of them affected the IOSurface kernel extension, and the other 7 weaknesses affected the AppleAVI Driver kernel extension.

The kernel kernel vulnerability helps the root exploit of the device

Even if Apple released the security patch, they also asked Donenfeld to complete the release of the exploit code to allow the user time to upgrade the device first.

Explaining the reasons for his research, Donenfeld said that he was 'trying to understand the kernel area that had never been thoroughly studied'. His research eventually led him to AppleAVE.

'AppleAVE is written but ignores basic security issues, the vulnerability described below is enough to occupy the kernel, random RW rights and root device', he said.

The code is exploited on GitHub

Donenfeld prepared a talk about these eight holes at the Singapore security conference - Hack In The Box. He works for Zimperium, the company discovered the famous Stagefright vulnerability on Android.

In February 2017, Zimperium introduced a program called N-Day, in which they proposed to buy zero-day vulnerabilities that were used and stopped working, avoiding public disclosure before patching. given. ZIVA exploit code is available on GitHub at this address.*https://github.com/doadam/ziVA*