



Issued 5/21/18

ZipperDown Affects 16,000 iOS Apps

These days, there seem to be two types of security vulnerabilities – those with alarming names and eye-catching logos, and those that make do with mere CVE numbers. The latest example of the naming trend is ZipperDown, uncovered by Chinese jailbreakers Pangu Lab, affecting iOS apps and possibly some Android ones too. The company offers only minimal detail on the flaw beyond, describing it as: "A common programming error, which leads to severe consequences such as data overwritten and even code execution in the context of affected apps." This sounds like trouble but this time the eye-catching bit is the number of apps the company believes might suffer from it – 15,978 (9.5%) of 168,951 iOS Apps in the App Store, a collection of computer programs that have been downloaded about 100 million times. They admit this is a guesstimate due to the impossibility of checking such a large number of apps individually. As for other platforms: "We have confirmed that many popular Android apps have similar issues. We will release more results for Android apps in future." As Pangu Lab alludes to in its advisory, exploiting it appears to require control of a Wi-Fi network, for example using a compromised public hotspot. That's not hard to imagine happening but still limits the chances of compromise for most users. The company also admits: "The sandbox on both iOS and Android can effectively limit ZipperDown's consequence."