Detecting an extremely dangerous vulnerability on nearly 16,000 iOS applications

Apps with high download volume and users of over 100 million people like Instagram, Amazon, Twitter and Dropbox are likely to be affected.

ZipperDown, a serious security vulnerability that exists in iOS apps, was discovered by a group of security experts called Pangu Lab. Taking advantage of this vulnerability, hackers can overwrite data or run dangerous code on the application. Users' devices may be in danger if downloaded one of the applications that has ZipperDown attached.

According to security experts, there are about 9,978 iOS applications that exist in the aforementioned flaws, accounting for about 10% of existing iOS applications on the App Store. Notably, apps with high download volume and users of over 100 million people like Instagram, Amazon, Twitter and Dropbox are likely to be affected by ZipperDown, while apps like Weibo, QQ Music, MOMO, NetEase Music, and Kwai, . have been identified as containing vulnerabilities long ago.

Depending on the application, hackers can exploit vulnerabilities to attack in different directions, but the most common is still control and fake connection to the device to enable remote malicious code via the network. cord.

Developers need to contact the Pangu team to verify if their application contains a vulnerability, thus finding a suitable solution.

See more:

1. Intel's chip has eight new serious vulnerabilities
2. Detecting zero-day vulnerabilities in Internet Explorer helps hackers gain control of the computer
3. Only charging the battery through a computer, your iPhone may also be hacked

You finished reading the article "**Detecting an extremely dangerous vulnerability on nearly 16,000 iOS applications**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.