Android exploits commanding higher price than ever before

Reference: Memo [190910-1] – Version: 1.0
Keywords: Android, iOS, exploit, vulnerability
Sources: Zerodium, Google, Wired

Key Points

- The price of android exploits exceeds the price of iOS exploits for the first time
- This is possibly because Android security is improving over iOS
- The release of Android 10 is also a likely cause for the price hike

Summary

Zerodium[1], a cyber security exploit broker dealing in zero-day vulnerabilities, has published its most recent price list. It indicates that the price of an Android full-chain exploit with persistence can fetch the developer up to 2,500,000 dollars. The going rate for a similar exploit for Apple's iOS has gone down by 500,000 dollars and is now worth 2,000,000. This is the first confirmed time when Android exploits are valued more than iOS.

Zerodium payouts for mobile devices		
Up to $2,500,000		Android zero click full compromise chain with persistence.
Up to $2,000,000		iOS zero click full compromise chain with persistence.
Up to $1,500,000	WhatsApp zero click remote code execution with local privilege escalation on iOS or Android.	iMessage remote code execution with local privilege escalation.
Up to $1,000,000	WhatsApp remote code execution with local privilege escalation on iOS or Android.	SMS/MMS remote code execution with local privilege escalation on iOS or Android.

Comments

Zero-click exploits do not require interaction from the user. This is very difficult to achieve and thus commands the highest prices. If the exploit has persistence, the compromised mobile device stays infected after it is rebooted or plausibly even re-installed. Again, this is more difficult to achieve because under normal circumstances this is achieved via user consent or elevated privileges. This is where local privilege escalation plays its role, allows adversaries to gain higher-level permissions on a computing device to achieve full control of the device.

There is a thriving market for operating system vulnerabilities and exploits. There are companies who specialise in buying exploits. Additionally, software manufacturers, such as Google, have bounty programs with payouts as high as $200,000[2] for critical flaws in their software. Still, security exploit brokers, such as Zerodium, are oftentimes the ones that pay the best price. These companies then sell them on to governments or other companies who manufacture cyber intrusion tools, such as FinFisher.

According to Chaouki Bekrar[3], CEO of Zerodium, there are many exploits for iOS available, which is driving down the price for new ones. At the same time, the security of the Android operating system is improving, reportedly thanks to mostly the efforts of Google and Samsung development teams. This, along with the release of the new and possible yet unbreached Android 10 operating system in early September 2019, is likely the cause for the price hike and the promise of record payouts.

Judging from Zerodium's dramatic increase in potential profits for cyber security bounty hunters, it is possible that other exploit buyers who do not publish their price lists are also willing to pay more for rare and difficult vulnerabilities.

[1] https://zerodium.com/program.html
[2] https://www.google.com/about/appsecurity/android-rewards/
[3] https://www.wired.com/story/android-zero-day-more-than-ios-zerodium/