**Hackers will Get Paid for Revealing Old Exploits by Mobile Security Firm**

A mobile security firm Zimperium has started a program that ask hackers to bring undisclosed attack codes for old exploits in the open and get paid for the job. This is being done to encourage optimal patching and boost mobile app security.

Though it might not seem like a fruitful idea to pay for old exploits, there are many business and technical arguments that validate this step. Many detected vulnerabilities in reality are reported to vendors without any working exploits. Vendors can usually understand the implications and do not always need exploits. They can patch the vulnerability on their own in this case. But this is not always that case. Many exploits are sold to hackers or government agencies behind closed doors, in exchange of a large sum of money. Such exploits are reliable and fully functional, and most of the times they target unpatched vulnerabilities which the users cannot guard for. Such exploits are known as zero-day exploits.

However, sometimes these exploits do not remain as zero-day exploits when the related vulnerabilities are discovered independently and the vendors patch them. They attack code in this case may or may not always get public.

Zimperium believes that by getting written exploits, it can direct itself towards better security for its partners and customers. Their mobile app security technology is used by handset vendors and carriers to cater to a large number of users. These also include users with older mobile devices which no longer get the security updates. Hence, old device support can teach them how to improve their services.

The firm is seeking exploits for remote and locally detected vulnerabilities, and also for bugs leading to information disclosure. Apart from latest versions, exploits can also target any Android or iOS versions. Zimperium will be using the mobile app security exploits to enhance its Z9 mobile application engine. Furthermore, the exploits will also be shared with ZHA, which consists of security team members from about 30 device manufacturers and carriers at global level.