ZERODIUM's Million Dollar iOS 9 Bug Bounty

You are here: Home (https://www.zerodium.com) » iOS Bounty

ZERODIUM iOS 9 BOUNTY

WANTED
REMOTE JAILBREAK
FOR iOS 9
ZERODIUM.COM
$1,000,000.00 REWARD
SUBJECT TO TERMS AND CONDITIONS
SEE ZERODIUM'S FULL ANNOUNCEMENT AND BOUNTY RULES

Sept. 21, 2015 - **ZERODIUM**, the premium zero-day acquisition platform, announces and hosts the world's biggest zero-day bug bounty program: **The Million Dollar iOS 9 Bug Bounty**.

Apple iOS, like all operating system, is often affected by critical security vulnerabilities, however due to the increasing number of security improvements and the effectiveness of exploit mitigations in place, Apple's iOS is currently the most secure mobile OS. But don't be fooled, secure does not mean unbreakable, it just means that iOS has currently the highest cost and complexity of vulnerability exploitation and here's where the Million Dollar iOS 9 Bug Bounty comes into play.

The Million Dollar iOS 9 Bug Bounty is tailored for experienced security researchers, reverse engineers, and jailbreak developers, and is an offer made by ZERODIUM to pay out a total of **three million U.S. dollars ($3,000,000.00)** in rewards for iOS exploits/jailbreaks.

ZERODIUM will pay out **one million U.S. dollars ($1,000,000.00)** to each individual or team who creates and **submits to ZERODIUM an exclusive, browser-based, and untethered jailbreak for the latest Apple iOS 9** operating system and devices.

The program is open until October 31st, 2015 at 6:00 p.m. EDT, and may be terminated prior to its expiration if the total payout to researchers reaches three million U.S. dollars ($3,000,000.00).

Eligibility / Conditions

➔ Eligible submissions must include a full chain of unknown, unpublished, and unreported vulnerabilities/exploits (aka zero-days) which are combined to bypass all iOS 9 exploit mitigations including: ASLR, sandboxes, rootless, code signing, and bootchain.

➔ The exploit/jailbreak must lead to and allow a remote, privileged, and persistent installation of an arbitrary app (e.g. Cydia) on a fully updated iOS 9 device (see below).

➔ The initial attack vector must be either:
- a web page targeting the mobile browser (Mobile Safari OR Google Chrome) in its default configuration; OR
- a web page targeting any application reachable through the browser; OR
- a text message and/or a multimedia file delivered through a SMS or MMS.

➔ The whole exploitation/jailbreak process should be achievable remotely, reliably, silently, and without requiring any user interaction except visiting a web page or reading a SMS/MMS (attack vectors such as physical access, bluetooth, NFC, or baseband are not eligible for the Million Dollar iOS 9 Bug Bounty. ZERODIUM may, at its sole discretion, make a distinct offer to acquire such attack vectors.).

➔ The exploit/jailbreak must support and work reliably on the following devices (32-bit and 64-bit when applicable):
- iPhone 6s / iPhone 6s Plus / iPhone 6 / iPhone 6 Plus
- iPhone 5 / iPhone 5c / iPhone 5s
- iPad Air 2 / iPad Air / iPad (4rd generation) / iPad (3th generation) / iPad mini 4 / iPad mini 2

➔ Partial or incomplete exploits/jailbreaks will not be eligible for the Million Dollar iOS 9 Bug Bounty. ZERODIUM may, at its sole discretion, make a distinct offer to acquire such partial exploits.

➔ All submissions must be made exclusively to ZERODIUM and must include the fully functioning exploit and its source code (if any), and a detailed whitepaper describing all the zero-day vulnerabilities and techniques used in the jailbreak.

Submissions / Acquisitions

All communications and/or submissions to ZERODIUM must be achieved through encrypted emails. ZERODIUM reserves the right to determine whether a submission is valid or not. Payment of the Million Dollar iOS 9 Bug Bounty by ZERODIUM to a researcher (individual or team) constitutes a purchase of the exclusive rights to the submitted exploit(s), jailbreak(s), and all related vulnerability information.

More information about ZERODIUM's premium exploit acquisition program is available in our FAQ (https://www.zerodium.com/faq.html).

For inquiries and/or submissions, please contact us using our PGP key (contact.html).

Home (https://www.zerodium.com) Program (https://www.zerodium.com/program.html)

iOS 9 Bounty (https://www.zerodium.com/ios9.html) FAQ (https://www.zerodium.com/faq.html)
Submit (https://www.zerodium.com/submit.html) About Us (https://www.zerodium.com/about.html)
Events (https://www.zerodium.com/events.html) Contact (https://www.zerodium.com/contact.html)