

New jailbreak tool unlocks almost all iPhones

26 May 2020, by Peter Grad



Credit: CC0 Public Domain

A new jailbreak tool that works on almost all iPhones in use today was released Saturday.

The renowned hacker group Unc0ver says its utility unlocks all iPhones running iOS 11 through iOS 13.5, which was released just last week.

Apple has long applied strict safeguards against the installation of apps it does not approve. But an aggressive hacker community that seeks the ability to install unauthorized apps and reshape the iPhone interface to personal preferences has continued to flourish.

Although jailbreaks in some instances can lead to malicious activity, researchers generally support jailbreak efforts because the expanded access such tools provide helps them better test security breaches and develop stronger protective measures.

Users who install jailbreak tools may enjoy enhanced customization but also risk stealth attacks from unvetted third-party sources.

The latest utility is the first one built on a zero-day vulnerability in years. Its lead developer, who goes by the name [Pwn20wnd](#), insists the jailbreak is stable and does not interfere with Apple's user data protections.

"This jailbreak basically just adds exceptions to the existing rules," Pwn20wnd [told](#) WIRED magazine. "It only enables reading new jailbreak files and parts of the file system that contain no user data."

Apple reports that 94 percent of iPhones currently have iOS 12 or iOS 13 installed. The jailbreak works on all of those models.

Such breaches are usually corrected soon after they are reported. Researchers estimate it will take Apple at least two to three weeks to fix the vulnerability, located in the kernel of the operating system.

While Apple has never supported jailbreaking tools, it has generally kept a hands-off approach to violators. In fact, it has brought two well-known hackers on board and has given recognition to others in release notes for new iOS versions.

Still, Apple has applied ever-more stringent barriers to jailbreaking utilities. As a result, a once flourishing hacker community specializing in unauthorized apps has greatly dwindled in recent years.

Nations around the globe handle the problem of jailbreaking tools differently. In 1996, the World Intellectual Property Organization Copyright Treaty required participating nations to combat digital rights management violations. Some have done so, but the United States, under the Digital Millennium Copyright Act, allows exemptions for non-copyright-infringing utilities such as jailbreaking tools. And European nations participating in the 2001 European Copyright Directive also have varying implementations of rules exempting jailbreaking

utilities.

Pwn20wnd sees the distribution of jailbreaking apps as a community service.

"Having a full-fledged jailbreak makes future security research easier," he said. As for his choice of Apple: "It's just a big target for attackers. Apple is constantly adding more features to iOS that introduce new attack surfaces."

© 2020 Science X Network

APA citation: New jailbreak tool unlocks almost all iPhones (2020, May 26) retrieved 19 June 2021 from <https://techxplore.com/news/2020-05-jailbreak-tool-iphones.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.