

Security researcher finds problems with iOS security vulnerabilities and Apple's response to them

September 27 2021, by Bob Yirka



Credit: Pixabay/CC0 Public Domain

An anonymous security researcher who goes by the name [illusionofchaos](#) has posted [a report](#) on the Russian-based IT blog Habr, describing four

zero-day vulnerabilities he found in Apple's latest iOS mobile operating system and his interactions with Apple's security bounty program representatives. In his post, he claims he discovered four vulnerabilities in iOS, three of which are outstanding and a fourth which he further claims was fixed but that he was not given credit for.

Apple started its [security](#) bounty program several years ago. The idea is that non-Apple employees can examine Apple's products and code and try to identify vulnerabilities. Security researchers who identify vulnerabilities are monetarily rewarded. Apple overhauled its program back in 2019, hoping to make it more accessible and to increase payouts to researchers. Unfortunately, the program has been receiving complaints from security researchers who claim that the team at Apple is difficult to reach. In this new effort, illusionofchaos suggests that Apple is putting its user base at risk by not making fixes to its new operating system that are found by researchers such as himself.

Illusionofchaos claims that the first vulnerability he found allowed user-installed apps to access iOS data without first being granted permission. He further claims that after sending Apple a report of his findings, he received messages suggesting the company would look into the issue. Later, he found that the issue has been resolved, but he was not credited with the find.

Illusionofchaos claims also that he has three other outstanding vulnerabilities he has reported to Apple. The first he calls gamed zero-day—he describes it as a [vulnerability](#) that exposes Apple ID email, name and other information. The second, which he calls Nehelper Wi-Fi zero-day, exposes Wi-Fi information. And the third, which he calls NeHelper Enumerate zero-day, allows interested parties to see information about apps that are installed on a device.

Illusionofchaos claims that he notified Apple about all three

vulnerabilities and received an initial response, but since then, has only received messages telling him that Apple is investigating the issue. After threatening to make the vulnerabilities public and still receiving no feedback, Illusionofchaos followed through with his threat by posting his findings on a blog. Apple has not yet publicly responded to the claims made by Illusionofchaos.

More information: habr.com/en/post/579714/

© 2021 Science X Network

Citation: Security researcher finds problems with iOS security vulnerabilities and Apple's response to them (2021, September 27) retrieved 13 March 2024 from <https://techxplore.com/news/2021-09-problems-ios-vulnerabilities-apple-response.html>

<p>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.</p>
--