Apple to fix FaceTime bug that allows eavesdropping

January 29 2019, by Matt O'brien And Carlo Piovano

In this Oct. 30, 2018, file photo Apple's new MacBook Air computers are displayed during the company's showcase of new products in the Brooklyn borough of New York. Apple Inc. reports earnings Tuesday, Jan. 29, 2019. (AP Photo/Bebeto Matthews, File)

Apple has disabled a group-chat function in FaceTime after users said a software bug could let callers activate another person's microphone remotely.

With the bug, a FaceTime user calling another iPhone, iPad or Mac computer could hear audio—even if the receiver did not accept the call. The bug is triggered when callers add themselves to the same call to launch a group chat. That makes FaceTime think the receiver had accepted the chat.

The bug, demonstrated through videos online , comes as an embarrassment for a company that is trying to distinguish itself by stressing its commitment to users' privacy.

"This is a big hit to their brand," said Dave Kennedy, CEO of Ohio-based security firm TrustedSec. "There's been a long period of time people could have used that to eavesdrop. These things definitely should be caught prior to ever being released."

There is no longer a danger from this particular bug as Apple disabled group chats, while regular, one-on-one FaceTime remains available.

NBC News and The Wall Street Journal reported Tuesday that the family of a 14-year-old high school student in Tucson, Arizona, tried to inform Apple about the bug more than a week before it became widely known to the public. The boy, Grant Thompson, said he discovered it by accident while calling friends to play the game "Fortnite."

In this Jan. 3, 2019 file photo, the Apple logo is displayed at the Apple store in the Brooklyn borough of New York. Apple has made the group chat function in FaceTime unavailable, Tuesday Jan. 29, 2019, after users said there was a bug that could allow callers to activate another user's microphone remotely. (AP Photo/Mary Altaffer, File)

It's hard to know if anyone exploited the bug maliciously, said Erka Koivunen, chief information security officer for Finnish company F-Secure. He said it would have been hard to use the bug to spy on someone, as the phone would ring first—and it's easy to identify who called.

Apple said Tuesday that a fix will come in a software update later this week. Apple declined to say when it learned about the problem. The company also wouldn't say if it has logs that could show if anyone took advantage of the bug before it became publicly known this week.

Kennedy commended Apple's quick response this week following reports of the bug by tech blogs. He predicted the reputational dent could soon be forgotten if it doesn't become part of a pattern.

"All bugs are obvious in retrospect," said Eva Galperin, director of cybersecurity at the Electronic Frontier Foundation. "The truth is bugs are subtle, code is complicated and sometimes things get through."

Galperin said Apple should develop a better process for fielding reports about potential security flaws. She said the 14-year-old's discovery of the problem "just tells us a lot about reporting security bugs depends on knowing the right person."

Apple had introduced the 32-person video conferencing feature in October for iPhones, iPads and Macs. Regular FaceTime calls aren't affected unless the caller turns it into a group chat.

Word of the bug came as Apple reported that profit for the last three months of 2018 dipped slightly to $20 billion while revenue fell 5 percent from the prior year to $84 billion. Earlier this month, Apple said that demand for iPhones was waning and that its earnings for the final quarter of 2018 would be below its own forecasts—a rare downgrade from the company.

© 2019 The Associated Press. All rights reserved.

Citation: Apple to fix FaceTime bug that allows eavesdropping (2019, January 29) retrieved 3 May 2024 from https://phys.org/news/2019-01-apple-group-facetime-bug.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.