

14-year-old's FaceTime bug discovery could rattle Apple

February 1 2019, by Matt O'brien



Grant Thompson and his mother, Michele, look at an iPhone in the family's kitchen in Tucson, Ariz., on Thursday, Jan. 31, 2019. The 14-year-old stumbled upon a bug in the iPhone's FaceTime group-chatting feature on Jan. 19 while calling his friends to play a video game. With the bug, a FaceTime group-chat user calling another iPhone, iPad or Mac computer could hear audio, even if the receiver did not accept the call. (AP Photo/Brian Skoloff)

At the heart of Apple's shocking FaceTime bug, which allowed just about anyone to turn an iPhone into a live microphone, stands a 14-year-old boy who stumbled upon the eavesdropping flaw more than a week before Apple took action.

"The thing that surprised me the most was that this glitch happened in the first place," said Grant Thompson, a high school freshman in Tucson, Arizona. "I'm only 14 and I found it by accident, instead of the people at Apple that get paid to find glitches."

Not only that, but Grant and his mom said they spent a week unsuccessfully trying to get Apple to do something about the bug in its FaceTime group-chatting feature. The bug allowed callers to activate another person's microphone remotely even before the person has accepted or rejected the call.

"It took nine days for us to get a response," he said. "My mom contacted them almost every single day through email, calling, faxing." Of the fax, he jokes, "I'm not even sure what that is. It's probably older than I am."

This eavesdropping scare is over now that Apple has disabled group chats, but the problem could dog the company for much longer. New York state officials have opened a consumer rights investigation. Others are raising questions about how long it took Apple to address the bug.

In a statement Friday, Apple thanked the Thompsons as it announced that it has identified a fix and will release it next week. FaceTime group chatting will resume then.

Grant, a straight-A student who plays basketball, does community volunteering and enjoys the video game "Fortnite," was calling friends to play the game on a Saturday night, Jan. 19, when he discovered the flaw.

"If a 14-year-old kid discovered it, I wonder how many other people discovered it," said Chris Wysopal, chief technology officer with the security firm Veracode.

Apple hasn't said whether it has records that could answer that question.

Friday's statement said Apple's engineers worked quickly once it got the details needed to reproduce the bug. Although Apple didn't acknowledge a delay, the company said it was "committed to improving the process by which we receive and escalate these reports, in order to get them to the right people as fast as possible."

The company—at first widely praised for its swift response—could come under increased scrutiny as regulators seek to learn more about the vulnerability.

New York Attorney General Letitia James and Gov. Andrew Cuomo said Wednesday that they're investigating "Apple's failure to warn consumers about the FaceTime bug and slow response to addressing the issue."

They said the bug jeopardized the privacy of New York consumers. James said her office's review will include a "thorough investigation into Apple's response."

Last October, Apple introduced the 32-person video conferencing feature for iPhones, iPads and Macs. With the bug, a FaceTime group-chat user calling another Apple device could hear audio—even if the receiver didn't accept the call. The bug was triggered when callers turned a regular FaceTime call into a group chat, making FaceTime think the receiver had accepted the chat.

In Grant's case, he had just gotten his Xbox ready and called to invite a

friend, Nathan, to play "Fortnite" with him online.

"You can swipe up and add another person, so I added another friend of mine, Diego, to see if he also wanted to play," he said. "But as soon as I added Diego, it forced Nathan to respond."

They were shocked at first, then tried to repeat the bug and it happened every time, he said. His mother, Michele Thompson, said she started trying to reach Apple the next day.

"They could have tested it within two minutes, realized it was true and brought it up the chain at Apple," said Thompson, who works as an attorney. "There needs to be a better process for the average citizen to report things like this. And a timelier response."

She eventually reached someone who advised that she could register as a software developer to submit the bug. Such reports can sometimes lead to "bug bounties" so that those who discover a flaw can get a financial reward. The family hoped Grant could receive such an award, or at least some credit, for his discovery.

"Every day he would ask me, 'Did we hear from Apple yet?' she said.

The family tried reaching Apple through multiple channels. They left comments on Twitter, one of them directed to CEO Tim Cook, and uploaded a video to walk Apple engineers through the problem. But it wasn't until a tech blog reported the flaw earlier this week—leading many people to experiment with the spying bug themselves—that Apple took the unusual measure of temporarily shutting down the group-chat feature.

Apple has 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. The company reached out to the Thompson family on Tuesday offering to give some public credit for their efforts, according to an email Michele Thompson shared with The Associated Press.

"It would be cool to just have Apple say thanks to me," Grant Thompson said before Friday's announcement from Apple. "And of course, the bug bounty, that would be pretty awesome to get, but as long as we got rid of this pretty groundbreaking bug, and Apple said thank you, that would be pretty cool."

© 2019 The Associated Press. All rights reserved.

Citation: 14-year-old's FaceTime bug discovery could rattle Apple (2019, February 1) retrieved 10 April 2024 from <https://phys.org/news/2019-02-year-old-facetime-bug-discovery-rattle.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>
--