Apple pushes fix for “FacePalm,” possibly its creepiest vulnerability ever



reader comments

46 with 31 posters participating

Share this story

Apple has patched one of its creepiest vulnerabilities ever—a flaw in its FaceTime messenger app that made it possible for people to eavesdrop on audio and video captured by iPhones and Macs.

The bug in Group FaceTime, a feature that allows conference-call-style chats, made it trivial for someone to eavesdrop on someone else simply by initiating a FaceTime call, swiping up and choosing “add person,” and entering their own number to add themselves as a participant in a Group FaceTime call.

While people on the receiving end would see a call was coming through, they would have no idea that the person trying to connect could already hear nearby audio and, in many cases, see video.

Two other potentially serious iOS security bugs Apple fixed Thursday have been under active attack in the wild, security researchers with Google's Project Zero said. One bug indexed as CVE-2019-7287, is a memory corruption flaw in the IOKit. Apple said it may allow apps to execute arbitrary code with kernel privileges. Another memory corruption bug in Foundation, CVE-2019-7286 may allow an application to gain elevated privileges.

The in-the-wild exploits could be severe because based on Apple's vulnerability description, they fundamentally subvert Apple's security model, which prevents apps from accessing other apps and from interacting with the security of iOS itself. A Google spokesman declined to provide details about the attacks. An Apple representatives also declined comment.

Apple security under the microscope

Privacy advocates and ordinary users were shocked when details of the eavesdropping vulnerability first broke 10 days ago. When it emerged that the bug was discovered by a 14-year-old and that Apple had failed to act following multiple emails sent by the teen's mother, people demanded answers. Since then, New York Attorney General Letitia James has launched a probe into the incident, according to Reuters. Some critics now refer to the bug as FacePalm.

On Thursday, Apple issued iOS and macOS updates here and here that fix the bug.

"A logic issue existed in the handling of Group FaceTime calls," the advisories stated. "The issue was addressed with improved state management."

Apple introduced Group FaceTime last year after some unexplained delays. Critics said the FacePalm vulnerability is evidence the new feature wasn't adequately tested prior to going live. The inability of the teenager's mother to reach someone at Apple who could grasp the seriousness of her son's discovery has opened Apple's security and quality assurance process to even more criticism.

Earlier this week, Apple security came under scrutiny again when an 18-year-old named Linus Henze posted a video discussing what he said was a weakness in macOS that needlessly exposes passwords stored in the keychain to malicious apps. While Henze didn't provide many details, he compared the weakness to a similar one disclosed in 2017 by former National Security Agency hacker Patrick Wardle.

[embedded content]
KeySteal – Stealing your keychain passwords on macOS Mojave.
While potentially serious, both keychain vulnerabilities can or could be exploited only after malicious software is already installed on a machine. This, in itself, is a high burden for most attackers. Apple fixed the vulnerability Wardle reported, but it's not clear if the newer vulnerability will ever be fixed. So far, Henze has declined to provide technical details to Apple, a move the teen says is intended to protest the company not having a bug-bounty program that covers macOS.

Update now

Once word of the FacePalm vulnerability became public, Apple disabled Group FaceTime on its servers. The move likely prevented anyone from further eavesdropping on unwitting users. Still, out of an abundance of caution, iOS and MacOS users should install the updates as soon as practical.

Updates are by default installed automatically but often not right away. Those who want to do so on iOS can choose Settings > General > Software Update and then choose Download and

Install. To manually install a macOS update, choose System Preferences > Software Update > and Download.

Post updated to add details about in-the-wild exploits.

https://arstechnica.com/?p=1453011