Apple fixes bug that could have given hackers full access to user accounts

reader comments

23 with 20 posters participating

Share this story

Sign in with Apple—a privacy-enhancing tool that lets users log into third-party apps without revealing their email addresses—just fixed a bug that made it possible for attackers to gain unauthorized access to those same accounts.

“In the month of April, I found a zero-day in Sign in with Apple that affected third-party applications which were using it and didn’t implement their own additional security measures,” app developer Bhavuk Jain wrote on Sunday. “This bug could have resulted in a full account takeover of user accounts on that third party application irrespective of a victim having a valid Apple ID or not.”

Jain privately reported the flaw to Apple under the company’s bug bounty program and received a hefty $100,000 payout. The developer shared details after Apple updated the sign-in service to patch the vulnerability.

Sign in with Apple debuted in October as an easier and more secure and private way to sign into apps and websites. Faced with a mandate that many third-party iOS and iPadOS apps offer the option to sign in with Apple, a host of high-profile services entrusted with huge amounts of sensitive user data

use adopted it.

Instead of using a social media account or email address, filling out Web forms, and choosing an account-specific password, iPhone and iPad users can tap an button and sign in with Face ID, Touch ID, or a device passcode. The bug opened users to the possibility their third-party accounts would be completely hijacked.

The sign-in service, which works similarly to the OAuth 2.0 standard, logs in users by using either a JWT—short for JSON Web Token—or a code generated by an Apple server. In the latter case, the code is then used to generate a JWT. Apple gives users the option of sharing the Apple email ID with the third party or keeping the ID hidden. When users hide the ID, Apple creates a JWT that contains a user-specific relay ID.

“I found I could request JWTs for any Email ID from Apple and when the signature of these tokens was verified using Apple’s public key, they showed as valid,” Jain wrote. “This means an attacker could forge a JWT by linking any Email ID to it and gaining access to the victim’s account.”

There’s no indication the bug was ever actively exploited.

https://arstechnica.com/?p=1680535