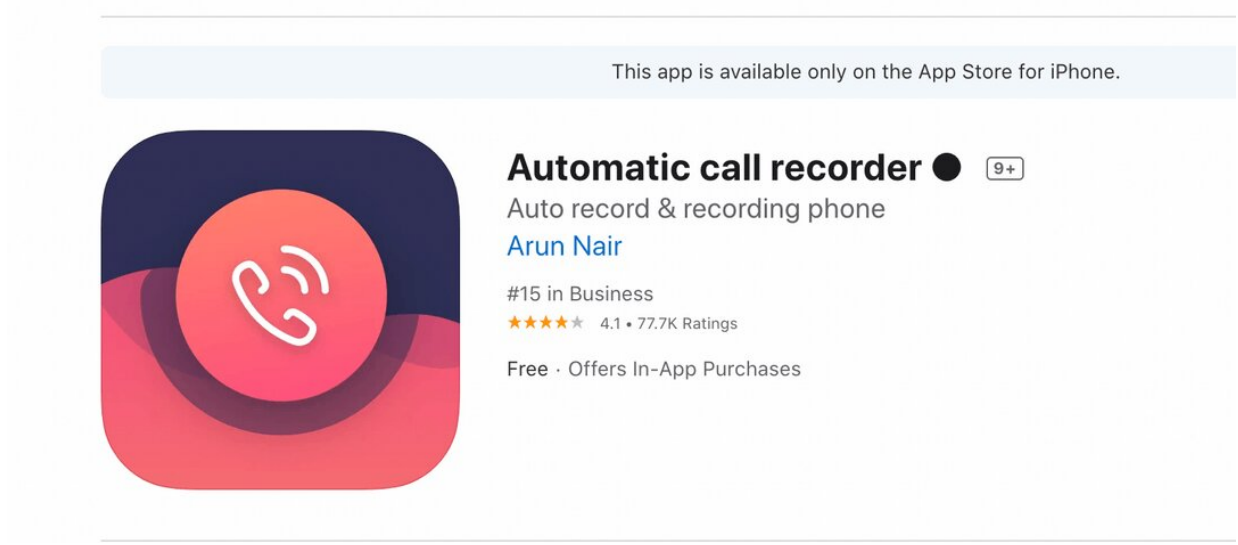
# Bug bounty company PingSafe AI discovers iPhone call recording app vulnerability

March 10 2021, by Sarah Katz




Call Recorder App. Copyright: PingSafe AI

PingSafe AI, a security company that monitors multiple breaches in real time, has uncovered a critical vulnerability in the iPhone automatic call recorder application that exposed thousands of users' recorded calls.

PingSafe works by assessing the security posture of an organization's domains, IPs, mobile applications, leaked credentials and source code. Discovered through open source intelligence by security researcher and PingSafe AI CEO, Anand Prakash, and verified by TechCrunch security

editor Zack Whittaker, this vulnerability allowed potential attackers to listen in on any call using the application's cloud storage bucket and an unauthenticated API endpoint that leaked the victim's cloud storage URL. In fact, PingSafe AI found that the application's IPA file even used host names, S3 buckets and other sensitive user data.

A malicious actor could exploit this vulnerability by substituting another user's number in the recordings request, prompting the API to respond with the storage bucket's recording URL without any authentication. All the attacker would need was the victim's phone number. Additionally, the app also displayed the victim's entire call history as well as numbers on which calls were made.

Prakash successfully uncovered this vulnerability using the application vulnerability testing program Burp Suite/ZAP, which showed him a POST API request to alter the victim's UserID to their phone number with any country code. At this point, the attacker could observe the victim's S3 URL along with further sensitive details.

While the Amazon Web Services cloud storage server was found to be open with the files inside exposed, the files could not be accessed or downloaded. Apple succeeded in closing the bucket in time for the press coverage of this vulnerability.

After recall and mitigation of this bug, a new version of the automatic call recorder application was released to the App Store on March 6, 2021. Undoubtedly, such vulnerabilities present immense risk for both users and businesses alike. On the user side, the customer stands to have a wealth of data exposed. On the other hand, the company that developed the application could suffer reputation damage and a significant loss of trust from both users and partners. Moreover, data leaked by these bugs can even provide an edge to brand competitors of organizations like Apple.

**More information:** Prakash, A. "How We Could Have Listened to Anyone's Call Recordings." PingSafe , PingSafe, 10 Mar. 2021, www.pingsafe.ai/blog/how-we-co … d04b0f7e8c9521f97343

Whittaker, Z. "A Bug in a Popular IPhone App Exposed Thousands of Call Recordings."TechCrunch, TechCrunch, 9 Mar. 2021, techcrunch.com/2021/03/09/ipho … usands-calls-exposed.