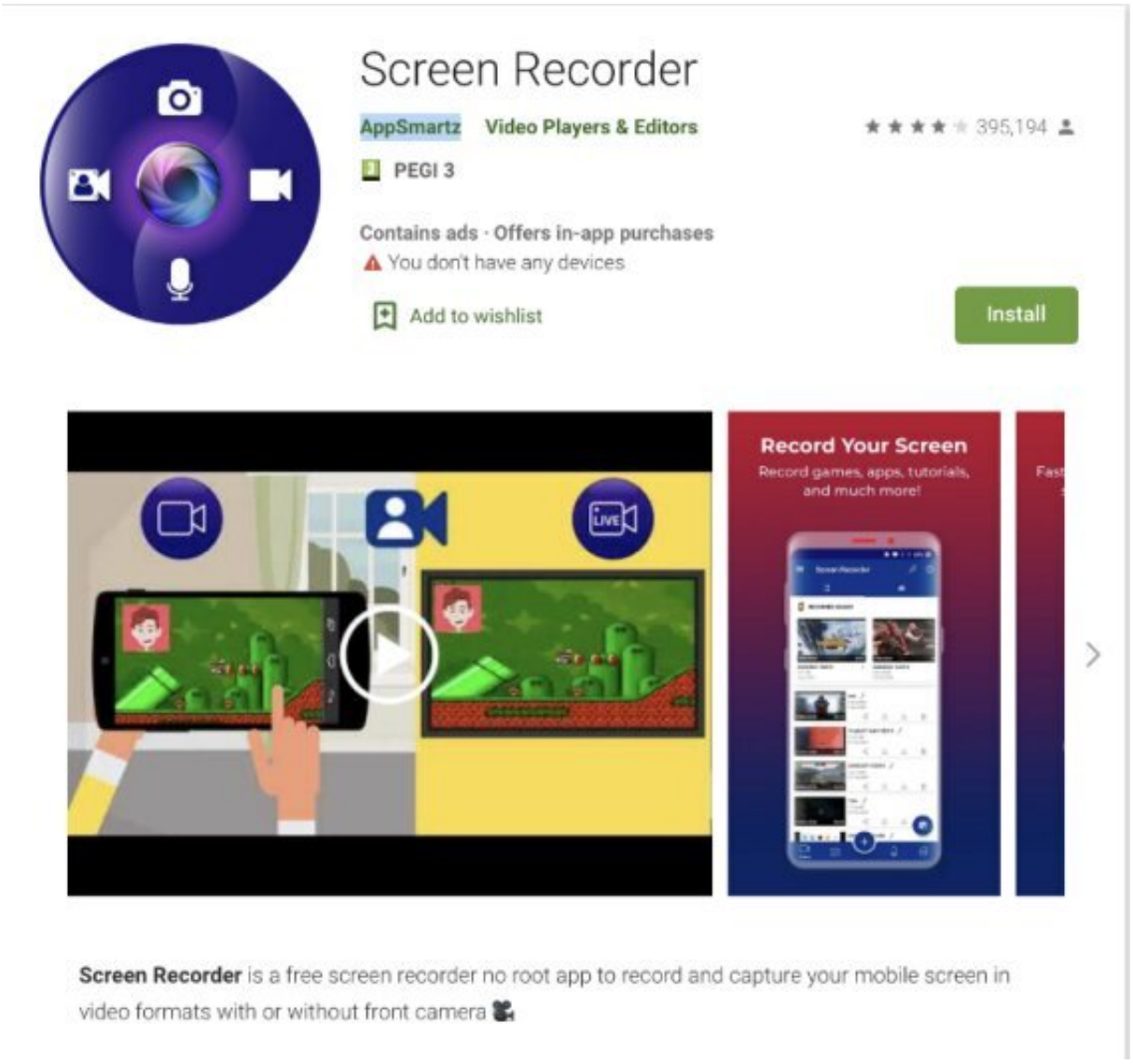
Misconfiguration of third party mobile apps exposes the data of 100 million users

May 21 2021, by Sarah Katz



Check Point Research backend code. Credit: Check Point Research

Despite the obvious benefits of contemporary cloud-based, mobile application development solutions—such as cloud storage, notification management, real-time databases, and analytics—many developers of these solutions fail to properly take into account the potential security risks involved when these apps are misconfigured.

Most recently, Check Point Research has discovered misconfigurations and implementation issues that have exposed the data of 100 million mobile application users. This kind of exposure places both the users as well as the app developers at risk of reputation threats and security damage. In this instance, the developers left open notification managers, storage locations and real-time databases to access by attackers, thus leaving 100 million users vulnerable.

In terms of real-time databases, cloud services can help mobile app users sync their data to the cloud in real time. However, when developers do not correctly implement this service with authentication, any user can theoretically access that database, including all mobile customer data. In fact, researchers expressed surprise at facing no obstacles to accessing these open databases for certain apps on Google Play. Some of the aspects obtainable in this case were device locations, email addresses, passwords, private chats and user identifiers, among other attack vectors. Such vulnerabilities leave all of these users at risk for fraud and identity theft.

Indeed, the popular horoscope app Astro Guru is one app with such vulnerabilities, potentially exposing all users to a leak of personally identifiable information (PII) – such as birthdate, email, gender and location as well as payment information—following a recorded 10 million downloads.

Similarly, the taxi app T'Leva which already has more than 50,000 installs allowed researchers to pull the full names of users as well as phone numbers and both destinations and intended pickup locations by sending just one request to the database.

Next, researchers also found that even the push notification manager had fallen vulnerable. This means that any malicious actor able to gain access to the manager could send the user notifications on the developer's behalf.

Moreover, cloud storage of these mobile apps presents a particular risk to users, as the research team also found that many developers left exposed both the access keys as well as the secret keys to stored data within the Screen Recorder service application. Evidently, a cursory analysis of the application file enabled researchers to recover these keys and access user recordings.

Finally, research showed that CopyCat malware also has the ability to retrieve keys for at-risk cloud storage services, demonstrating how malicious developers can also take advantage of these vulnerabilities.

More information: Hazum, A., et al. "Mobile App Developers' Misconfiguration of Third Party Services Leave Personal Data of over 100 Million Exposed." Check Point Research, Check Point Research, 20 May 2021, research.checkpoint.com/2021/m … 100-million-exposed/.