Lookout App Security Assessment

Comprehensive mobile app analysis

Overview

Understanding the security risks a mobile app poses requires both expertise and app intelligence to enable data-driven analyses that put risks in context and identify complex, hidden vulnerabilities.

Lookout App Security Assessment leverages Lookout's massive app intelligence dataset of over 30 million apps and couples it with the analysis power of Lookout's top security researchers to deliver the industry's most comprehensive app security risk assessment report.

What You Get

A Lookout App Security Assessment report summarizes the relevant, actionable results of Lookout's machine intelligence and researcher-driven analyses:

- **Code Construction Analysis -** Insight into the libraries, encryption and obfuscation techniques of a given application.
- **Permission & Behavior Analysis -** Detailed documentation of an app's data access capabilities and activities, including invisible background behaviors.
- **Vulnerability Analysis -** Apps are reviewed for all classes of vulnerability in the mobile OWASP Top Ten, including code errors, design flaws, and business logic issues. This includes both known and zero-day vulnerabilities.
- **Network Traffic Analysis -** Enumeration and analyses of the endpoints the app communicates with and the data transmitted.
- **Prevalence Analysis -** Understand the relative popularity of a given application and its prevalence in key operational geographies.
- **Malware Analysis -** Lookout checks every app for malware using advanced correlative analysis drawing on its 30 million+ app corpus.

Benefits

Smarter Risk Management

Make informed decisions about the risk of deploying third-party or internally-developed apps within your organization; block apps that may pose an unacceptable level of security risk to organizational data and systems (until the identified vulnerabilities are remediated).

Enhance App Risk Awareness

A Lookout App Security Assessment Report includes detailed information about app authorship and prevalence data, such as a list of apps that share that application's signer, which can enable you to investigate and manage risk at a policy-driven level based on shared app characteristics.

Brand Protection

Organizations that develop customer facing apps can use Lookout App Security Assessment to ensure the apps they develop are free of malware, vulnerabilities, and data risk imposed by app behaviors, preventing app-based privacy and security breaches that could negatively impact an organization's brand reputation.

In-Depth Look: Vulnerability Analysis

A Lookout App Security Assessment includes a comprehensive review of the mobile application for both known vulnerabilities and zero-day vulnerabilities. Lookout analysts will summarize vulnerability findings in a table such as the one displayed in Figure 1 below:

Figure 1: Mobile App Vulnerability Summary Table

Vulnerability Summary

Vulnerability	Risk	Ease of exploit
Account compromise via session fixation	HIGH	MEDIUM
Inadequate security controls against brute force attacks	HIGH	TRIVIAL
Disclosure of attacker specified files on the device via XML external entities	HIGH	DIFFICULT
SSL certificate pinning not implemented	HIGH	DIFFICULT
Information disclosure of user email address and device information	MODERATE	TRIVIAL
Application Transport Security explicitly disabled	MODERATE	N/A
Server infrastructure appears to contain known vulnerabilities	MODERATE	N/A
Information disclosure of user flight queries	LOW	TRIVIAL
Precise device location tracked by application and passed to remote server	INFO	N/A
Application has access to device contacts	INFO	N/A
Application has access to user's calendar	INFO	N/A

Each vulnerability in the summary table is then discussed in multi-page written analyses that may include screenshots of relevant vulnerable code, user interfaces, and even theoretical attacker code that could be used to exploit a given vulnerability, such as a script an adversary could use to obfuscate an email addresses to be a value that an app's host servers would expect, thereby enabling a brute force attack against that account.

Lookout empowers your organization to adopt secure mobility without compromising productivity by providing the visibility IT and security teams need. To learn how you can secure your mobile fleet today, contact us at sales@lookout.com.