



Vetting the Security of Mobile Applications

Recently, organizations have begun to deploy mobile applications (or apps) to facilitate their business processes. Such apps have increased productivity by providing an unprecedented level of connectivity between employees, vendors, and customers, real-time information sharing, unrestricted mobility, and improved functionality. Despite the benefits of mobile apps, however, the use of apps can potentially lead to serious security issues. This is so because, like traditional enterprise applications, apps may contain software vulnerabilities that are susceptible to attack. Such vulnerabilities may be exploited by an attacker to gain unauthorized access to an organization's information technology resources or the user's personal data.

To help mitigate the risks associated with app vulnerabilities, organizations should develop security requirements that specify, for example, how data used by an app should be secured, the environment in which an app will be deployed, and the acceptable level of risk for an app. To help ensure that an app conforms to such requirements, a process for evaluating the security of apps should be performed. NIST refers to this process as an app vetting process. An app vetting process is a sequence of activities that aims to determine if an app conforms to an organization's security requirements. An app vetting process comprises two main activities: app testing and app approval/rejection. The app testing activity involves the testing of an app for software vulnerabilities by services, tools, and humans to derive vulnerability reports and risk assessments. The app approval/rejection activity involves the evaluation of these reports and risk assessments, along with additional criteria, to determine the app's conformance with organizational security requirements and ultimately, the approval or rejection of the app for deployment on the organization's mobile devices.

The purpose of this document is to help organizations understand the process for vetting the security of mobile applications, plan for the implementation of an app vetting process, develop app security requirements, understand the types of app vulnerabilities and the testing methods used to detect those vulnerabilities, and determine if an app is acceptable for deployment on the organization's mobile devices.

The attached zip file includes:

- Intro Page.pdf
- Terms and Conditions.pdf
- Vetting Security Mobile Apps.pdf