ReedSmith

Cyber Security Agency of Singapore publishes updated Safe App Standard

13 November 2024

Key takeaways

- The Cyber Security Agency of Singapore published an updated standard to enhance mobile app security and safeguard high-risk transactions and user data.
- App developers and owners in Singapore are encouraged to adopt SAS 2.0 to fortify apps against common attacks and instil greater confidence in app transactions.

Authors: Bryan Tan Hannah Kong Eng Han Goh (Resource Law LLC)

Introduction

The Cyber Security Agency of Singapore (CSA) recently unveiled version 2.0 of its Safe App Standard (SAS), marking a significant step forward in mobile application security for developers and tech businesses. This update is particularly relevant for high-risk apps, such as those handling financial transactions, where security lapses could result in considerable financial losses.

Mobile apps are widely used in Singapore for various purposes, such as banking, e-commerce and government services. However, they also pose significant security risks, as they handle sensitive data and perform high-risk transactions that could result in financial losses or data breaches. To address these risks, CSA published the first version of the SAS in January 2024.

New security controls

SAS 2.0 introduces four new key areas of security controls, which are essential to protect data communicated between the app and servers, ensure the confidentiality and integrity of data stored on devices, detect and mitigate software vulnerabilities and coding bugs, and prevent exploitation of platform features. The four new areas are:

1. Network communication: This area covers the encryption of data transmitted by apps with secure protocols, such as Transport Layer Security, and the verification of server certificates to ensure data is sent only to trusted servers.
2. Cryptography: This area covers the use of strong cryptographic algorithms, such as the Advanced Encryption Standard, and digital signatures, such as the Elliptic Curve Digital Signature Algorithm, to encrypt and authenticate data stored on devices. It also covers the secure management of

cryptographic keys, such as using hardware-backed key stores or trusted execution environments, to minimise the risk of compromise.

3. Code quality and exploit mitigation: This area covers the review and testing of software libraries and developer code before use, and the adherence to secure coding practices, such as input validation and output encoding. It also covers the implementation of exploit mitigation techniques, such as address space layout randomisation and stack canaries, to prevent attackers from executing malicious code or exploiting memory corruption vulnerabilities.
4. Platform interactions: This area covers the security measures for operating system features, such as keyboards and in-app links, which can be used by attackers to inject malicious code or extract data. It also covers the use of platform-specific security mechanisms, such as Android App Bundles and iOS App Transport Security, to ensure apps run only on secure platforms and comply with platform policies.

Conclusion

App developers and owners should familiarise themselves with the requirements and guidelines of SAS 2.0. Although it is a voluntary standard, compliance will be a competitive advantage that demonstrates to users that the apps they use are part of a more secure digital landscape they can trust for their digital transactions.

Reed Smith LLP is licensed to operate as a foreign law practice in Singapore under the name and style Reed Smith Pte Ltd (hereafter collectively, "Reed Smith"). Where advice on Singapore law is required, we will refer the matter to and work with Reed Smith's Formal Law Alliance partner in Singapore, Resource Law LLC, where necessary.