M2: Inadequate Supply Chain Security

Threat Agents

Application Specific

An attacker can manipulate application functionality by exploiting vulnerabilities in the mobile app supply chain. For example, an attacker can insert malicious code into the mobile app's codebase or modify the code during the build process to introduce backdoors, spyware, or other malicious code.

This can allow the attacker to steal data, spy on users, or take control of the mobile device. Moreover, an attacker can exploit vulnerabilities in third-party software libraries, SDKs, vendors, or hardcoded credentials to gain access to the mobile app or the backend servers.

This can lead to unauthorized data access or manipulation, denial of service, or complete takeover of the mobile app or device.

Attack Vectors

Exploitability AVERAGE

There are multiple ways to exploit Inadequate Supply Chain vulnerability for example- an insider threat

agent or an attacker can inject malicious code during the development phase of the app, then they can compromise the app signing keys or certificates to sign malicious code as trusted.

Another way, a threat agent can exploit vulnerabilities in third-party libraries or components used in the app.

Security Weakness

Prevalence COMMON

Detectability DIFFICULT

Inadequate Supply Chain vulnerability occurs due to a lack of secure coding practices, insufficient code reviews and testing leading to the inclusion of vulnerabilities in the app.

Other causes for inadequate supply chain vulnerabilities include insufficient or insecure app signing and distribution process, weakness in third-party software components or libraries, insufficient security controls for data, encryption, storage, or exposing sensitive data to unauthorized access.

Technical Impacts

Impact SEVERE

If an attacker successfully exploits inadequate supply chain security, the technical impact can be severe. The specific technical impact depends on the nature of the exploit, but it can include:

Data Breach: The attacker can steal sensitive data, such as login credentials, personal data, or financial information. The data breach can have long-term consequences for the affected individuals, such as identity theft or financial fraud.

Malware Infection: The attacker can introduce malware into the mobile application, which can infect the user's device and steal data or perform malicious activities. The malware can be difficult to detect and remove, and it can cause significant damage to the user's device and data.

Unauthorized Access: The attacker can gain access to the mobile application's server or the user's device and perform unauthorized activities, such as modifying or deleting data. This can result in data loss, service disruption, or other technical issues.

System Compromise: The attacker can compromise the entire system of the mobile application, which can lead to a complete loss of control over the system. This can result in the shutdown of the application, significant data loss, and long-term damage to the reputation of the mobile application developer.

Business Impacts

Impact SEVERE

If an attacker successfully exploits inadequate supply chain security, the business impact can be significant. The specific business impact depends on the nature of the exploit and the organization's size, industry, and overall security posture, but it can include:

Financial Losses: The organization can suffer financial losses as a result of the attack, such as the cost of investigating the breach, the cost of notifying affected individuals, or the cost of legal settlements. The organization can also lose revenue if customers lose trust in the mobile application and stop using it.

Reputational Damage: The organization can suffer reputational damage as a result of the attack, which can lead to long-term damage to the organization's brand and customer trust. This can result in reduced revenue and difficulty in attracting new customers.

Legal and Regulatory Consequences: The organization can face legal and regulatory consequences as a result of the attack, such as fines, lawsuits, or government investigations. These consequences can result in significant financial and reputational damage to the organization.

Supply Chain Disruption: The attack can disrupt the organization's supply chain and lead to delays or interruptions in the delivery of goods or services. This can result in financial losses and reputational damage to the organization.

Am I vulnerable to 'Inadequate Supply Chain Vulnerability'?

It is possible that you are vulnerable to inadequate supply chain vulnerability, particularly if you use mobile applications that are developed by third-party developers or rely on third-party libraries and components. The vulnerability can arise due to a variety of reasons, such as:

Lack of Security in Third-Party Components: Third-party components, such as libraries or frameworks, can contain vulnerabilities that can be exploited by attackers. If the mobile application developer does not vet the third-party components properly or keep them updated, the application can be vulnerable to attacks.

Malicious Insider Threats: Malicious insiders, such as a rogue developer or a supplier, can introduce vulnerabilities into the mobile application intentionally. This can occur if the developer does not implement adequate security controls and monitoring of the supply chain process.

Inadequate Testing and Validation: If the mobile application developer does not test the application thoroughly, it can be vulnerable to attacks. The developer may also fail to validate the security of the supply chain process, leading to vulnerabilities in the application.

Lack of Security Awareness: If the mobile application developer does not have adequate security awareness, they may not implement the necessary security controls to prevent supply chain attacks.

How Do I Prevent 'Inadequate Supply Chain Vulnerability'?

- Implement secure coding practices, code review, and testing throughout the mobile app development lifecycle to identify and mitigate vulnerabilities.
- Ensure secure app signing and distribution processes to prevent attackers from signing and distributing malicious code.
- Use only trusted and validated third-party libraries or components to reduce the risk of vulnerabilities.
- Establish security controls for app updates, patches, and releases to prevent attackers from exploiting vulnerabilities in the app.
- Monitor and detect supply chain security incidents through security testing, scanning, or

other techniques to detect and respond to incidents in a timely manner.

Example Attack Scenarios

Scenario #1 Malware Injection

An attacker injects malware into a popular mobile app during the development phase. The attacker then signs the app with a valid certificate and distributes it to the app store, bypassing the app store's security checks. Users download and install the infected app, which steals their login credentials and other sensitive data. The attacker then uses the stolen data to commit fraud or identity theft, causing significant financial harm to the victims and reputational damage to the app provider.

References

- OWASP
  - Supply Chain Vulnerabilities
  - OWASP Dependency Check
- External
  - External References

Edit on GitHub

Spotlight: Guardsquare

GUARDSQUARE
Mobile application protection

Guardsquare offers the most complete approach to mobile application security on the market. Guardsquare's software integrates seamlessly across the development cycle: from app security testing to code hardening to real-time visibility into the threat landscape. Guardsquare products provide enhanced mobile application security from early in the development process through publication. More than 900 customers worldwide across all

major industries rely on Guardsquare to help them identify security risks and protect their mobile applications against reverse engineering and tampering. Learn more at www.guardsquare.com.

Corporate Supporters

Become a corporate supporter