



2020 SOURCE CODE USER PRIVACY ASSESSMENT

Mintegral

December 21, 2020
BDO Digital

Contents

EXECUTIVE SUMMARY	2
Prepare the Organization (PO).....	6
Protect the Software (PS)	10
Produce Well-Secured Software (PW)	17
Respond to Vulnerabilities (RV)	21

Figures

<i>Figure 1, SDK Versions</i>	10
<i>Figure 2, iOS SDK Process Flow</i>	12
<i>Figure 3, Information Collected</i>	13
<i>Figure 4, Vulnerability/Remediation Timeline</i>	23

EXECUTIVE SUMMARY

BDO Digital, LLC (BDO) is pleased to submit to Mobvista the third-party source code user privacy assessment (“Assessment”) of the Mintegral platform.

BDO’s work plan and methodology were based upon our understanding of Mintegral’s operational infrastructure, our prior industry experience, and fieldwork performed.

Due to the ongoing COVID-19 pandemic, BDO conducted activities remotely with the assistance of Mobvista’s Vice President of Global Strategic Initiatives, who provided BDO with access to source code repositories so that BDO could conduct its review and Assessment. Meetings and interviews were conducted via video conferencing applications.

During the Assessment, BDO focused on comprehensive testing and review of the Mintegral platform. This review included Mintegral’s existing governance models, information technology architecture, physical and logical security posture, reporting structure, process improvements, target-state architecture, and records within associated data sets to examine alignment and compliance with appropriate privacy standards and Secure Software Development Framework (SSDF). As part of our Assessment, BDO conducted interviews of key personnel directly responsible for development and release of the software platform.

Comprehensive assessments can be found within their respective sections of this report.

As is always the case, BDO may learn information subsequent to the release of this report that implicates information in within. When that happens, BDO reserves the right to amend the report if necessary.

BDO welcomes any comments or further inquiry regarding our findings and/or conclusions.

Sincerely,



Michael Barba, CISSP, GSNA, DFCE, EnCE, CPP
Practice Leader - National Security Compliance
Managing Director
BDO USA, LLP

Compliance Review Objective

BDO’s review concentrated on assessing Mintegral’s software platform and determining whether the existing and enhanced policies and governance models established and

maintained as part of its enterprise data privacy standards in addition to the software architecture and methods utilized in its platform conform to the Secure Software Development Framework.

Assessment objectives included, but were not limited to:

- ▶ Providing an independent assessment of Mintegral’s software platform and opining on its posture related to data privacy standards.
- ▶ Acquiring all relevant and necessary evidence including: documentation, data, and information to determine whether the policies, procedures, and processes at Mintegral that were either created, amended or already in place as part of efforts to ensure data privacy standards.
- ▶ Performing focused evaluation and testing of privacy and control procedures at Mintegral to identify any areas with gaps that allow for potential breach with the privacy standards and assess remediation activities, if any, as appropriate.
- ▶ Conducting interviews with subject matter experts directly responsible for source code development and release, as well as other key personnel responsible for the development and implementation of policies and procedures designed to provide governance within their respective business units.
- ▶ Performing review and testing procedures remotely as applicable.

Methodology & Assessment

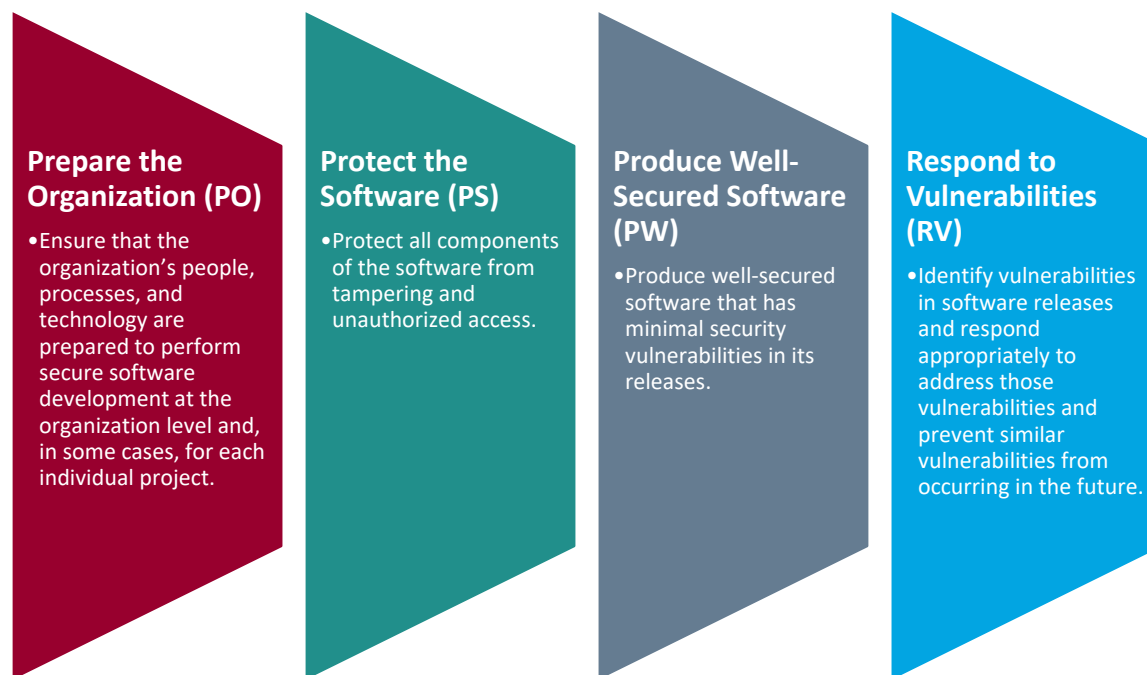
BDO utilized compliance-based sampling considerations to determine the sample size necessary to assess the sufficiency of evidence supporting this Assessment. The sample testing performed, as applicable, included risk-based sampling, population-based sampling, ratio or attribute sampling, or full-population testing.

SOURCE CODE IN-SCOPE SYSTEMS

To assess Mintegral’s software security posture and software development framework, BDO performed a review and analysis of the following:

- ▶ iOS GitHub Repositories
- ▶ Android GitHub Repositories

BDO’s source code review focused on potential vulnerabilities as well as identifying any potential methods either storing and/or transmitting Personally Identifiable Information (PII). Overall, BDO’s review, testing, and methodology were guided by the National Institute of Standards and Technology’s cyber security whitepaper, *Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)*. The framework identifies four key areas that will be most helpful to organizations that wish to adhere to a SSDF, and this Assessment is organized based on those four key areas:



Lastly, BDO aligned the source code to the privacy policies set forth in the App Store and Google Play Store.

For avoidance of doubt regarding this Assessment, BDO neither compiled nor executed Mintegral’s iOS and Android SDKs in order to assess each for vulnerabilities in a simulated operational environment. The goal of the Assessment was to provide an opinion regarding Mintegral’s development cycle relative to the aforementioned SSDF.

Interviews of Key Personnel

As part of the Assessment, BDO conducted video and telephonic interviews with members of Nativex/Mintegral’s executive team, corporate security personnel, and key personnel directly responsible for development and implementation of the source code.

Interviews focused on the specific areas of responsibility of each interviewee, as well as relevant questions specific to points of interest throughout the Assessment.

These interviews, as well as an examination of Mintegral’s policies and procedures and their implementation and practical application, provided the foundation for BDO’s evaluation of Mintegral’s software privacy standards. A listing of interviews follows.

Interview Subject(s)	Interview Topic	Application	Date
▶ Mr. Magneto Wu—Group Vice President ▶ Members of the SDK Development Team	Software development	Platform development; Security; Governance	November 18, 2020

Interview Subject(s)	Interview Topic	Application	Date

Assessment Conclusions

BDO has gained an appropriate level of confidence regarding the findings, conclusions and recommendations reached within the Secure Software Development Assessment.

Based on the results of BDO’s Assessment, Mintegral’s governance model, monitoring program, and logical security posture, are sufficient to facilitate secure software development. Mintegral has instituted or adopted from Mobvista a comprehensive suite of policies establishing governance, in particular, in the areas of securing software as well as collection and transmission of Personally Identifiable Information and other sensitive information. BDO did note one (1) Area for Improvement; however, this item may be easily remedied in future releases and is not impactful enough to render an opinion of insufficient.

BDO’s assessment, determinations, and recommendations follow.

Secure Software Development Matrix

The Secure Software Development Matrix provides a snapshot of the Assessment status. Further detail regarding each Assessment may be found under the appropriate section of this report.

Key

Symbol	Meaning
●	Not Applicable
●	Unsatisfactory
●	Area for Improvement
●	Acceptable

Matrix

#	Key Areas	Assessment
1	Prepare the Organization (PO)	●
2	Protect the Software (PS)	●
3	Produce Well-Secured Software (PW)	●
4	Respond to Vulnerabilities (RV)	●

PREPARE THE ORGANIZATION (PO)

Assessment Opinion

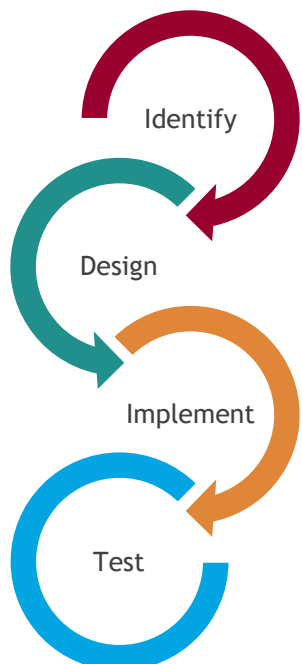
Practice	Assessment
PO	●

OVERVIEW

BDO’s assessment relative to secure software development was to identify if Mintegral develops and employs appropriate governance over secure software development, data security, and data privacy concerns with corporate policies and controls.

Secure Software Development

BDO conducted a review of Mintegral’s corporate security policies—either created by Mintegral or adopted from Mobvista—and evaluated the adequacy of controls embedded within the policies. BDO noticed in the *Software Development Safety Management Guidelines*, Mintegral has established numerous controls on security measures in its software development life cycle, which align with the security-by-design approach:



Methodology & Assessment

- ▶ Conduct interviews with Mobvista/Mintegral key stakeholders to determine organizational preparation to perform secure software development
- ▶ Review organizational policies including, but not limited to:
 - Information Security policy
 - Cyber Security Policy
 - Data Retention Policy
- ▶ Review any applicable training relative to secure software development
- ▶ Review organizational structure to assess rolls are appropriately defined in the software development life cycle (development, quality assurance, release management, etc.)

Identify

The process starts with conducting a risk assessment of the software development project by identifying software security requirements.

Design

The identified security requirements determine software architecture and module design to ensure appropriate security measures can be implemented. The policy also defines fundamental security requirements for a secure software design and implementation to establish consistency and facilitate code security.

Implement

The implementation phase includes various processes on reviewing and testing the source code to ensure security objectives are met. To ensure coding consistency, Mintegral established coding principles and standards for all programmers. BDO reviewed a copy of the JAVA Coding Principles and Specifications for Android Development and found the document adequately provides coding standards to ensure consistency in code implementation. BDO's source code review also found evidence that the coding standard is followed during the implementation of the Mintegral Software Development Kit (SDK). Additionally, BDO noted that Mintegral's *Code Security Development Management Measures* policy provides principles of safe and secure programming guidelines covering common security threats and vulnerabilities in mobile programming.

Test

The final phase of the secure software development is to conduct numerous tests to ensure the software implementation satisfies the design's security requirements. BDO found Mintegral's testing procedures to be appropriate to uncover any deficiency in the security requirements.

BDO further evaluated the security posture of the software development environment and applicable policies and controls governing the use and maintenance of the development environment. Mintegral's *Internal Audit of the Information Security Management System* policy states that security inspections of information system are conducted on a monthly basis.


Data and Privacy Protection Policy

Mintegral's Data Security Management Measures policy states that Mintegral shall disclose the types of information collected from users using or accessing its systems. BDO noted that Mintegral's *Privacy Policy*, which is available to the public on its website (<https://www.mintegral.com/en/privacy/>), provides a list of information that Mintegral may collect from users who interact with advertising services. The same information is also found in multiple pages within Mintegral's website describing its SDK, advertising services and use of user information. The listing of user information published on Mintegral's website follows.

- ▶ Device make, device model, operating system (e.g. iOS) and the OS version of the device, device type (e.g. smartphone, tablet, etc.);

- ▶ Screen size, orientation and battery
- ▶ Carrier information
- ▶ Version and characteristic of the app used by you when you interact with Mintegral's Service, Country, time zone and locale settings (country and preferred language)
- ▶ Network connection type, Network status such as Wi-Fi
- ▶ Internet Protocol (IP) address
- ▶ SDK version
- ▶ Timestamp
- ▶ Identifier for advertiser (e.g. IDFA)
- ▶ Device event information such as crashes, system activity, hardware settings
- ▶ The date and time of your request and referral URL
- ▶ User-agent
- ▶ Package name of the app of Mintegral's business partners
- ▶ Identifier for Vendors (IDFV)
- ▶ System file size, system update time, system boot time
- ▶ Device username
- ▶ Random access memory (RAM), remaining available RAM, CPU version
- ▶ International mobile equipment identity (IMEI) and Android ID solely for mainland China

BDO reviewed the list of user data and conducted an interview with Mintegral's SDK development team to gain an understanding of the purpose of collecting such data. BDO learned that Mintegral uses the information during its attribution process and some information is required to share with its partners to provide interactive ad experiences on the users' devices and reconcile ad delivery statistics. The *Privacy Policy* states:



“Where required, our business partners (e.g. publishers) will obtain User consent for and on our behalf for our processing of User personal information for profiling and displaying ads, including personalized ads or behavioral ads, on a User’s device. A User can withdraw their consent at any time.”

Privacy Policy Section 4, How We Use Users’ Personal Information

Mintegral’s SDK does not directly interact with the mobile device users, instead, the publishers’ mobile applications implementing the SDK would require obtaining the users’ permission for accessing the users’ personal information on the device.

BDO further noted that Mintegral’s mobile ad platform is certified annually by the kidSAFE Seal Program for satisfying the requirements outlined in the Children’s Online Privacy Protection Act (COPPA).

Based on the security policies, Mintegral utilizes encryption, network segmentation, firewall and other security technologies to protect user data on its information systems. BDO also noted in the *Data Retention* policy that Mintegral “... will only keep this personal information for no less than two (2) years.” The retention period depends on the regulatory requirements, contractual arrangements, and other similar obligations.

CONCLUSIONS

Based on the foregoing, BDO has determined that Mintegral’s control posture for Prepare the Organization (PO) is **ACCEPTABLE**. Mintegral’s security policies, software development guidelines and procedures, as well as coding standards ensure the organization and its employees are prepared to perform secure software development.

PROTECT THE SOFTWARE (PS)

Assessment Opinion

Practice	Assessment
PS	●

OVERVIEW

On October 28, 2020, BDO obtained a copy of Mintegral’s open-source SDK for iOS and Android systems from Mintegral’s secure website, which is only made available to registered users on the site. The downloaded open-source SDK version numbers and the number of files are shown in the table below:

System	SDK Version ¹	File Count	Size
iOS	6.6.5	546	14.6 MB
Android	15.1.0	894	6.96 MB

Figure 1, SDK Versions

BDO conducted an interview with the Mintegral SDK development team to gain an understanding of the development environment and processes. Mintegral utilizes Git as its source code repositories, which is housed within Mintegral’s information technology infrastructure. As noted in the security policies, for software development security reasons, access to the repositories is restricted to personnel who work on the development to ensure the security of the development projects.

SOURCE CODE REVIEW - iOS SDK

Mintegral’s open-source iOS SDK comes with the Xcode project and workspace files, which allow developers to easily incorporate into

¹ BDO notes that its Assessment only applies to the SDK versions listed in this table and the determinations of this assessment may not be applicable to any previous or subsequent version.

Methodology & Assessment

- ▶ Perform source code reviews of the Mintegral platform for both iOS and Android versions to determine if the software is protected from tampering and unauthorized access
- ▶ Review all source code repositories to determine access is restricted based on the policy of least privilege
- ▶ Review all repositories to determine if software releases are securely archived with access restricted

existing projects. The iOS SDK project contains a total of 546 files including 245 classes implemented in Objective-C, an object-oriented programming language designed to interact with devices running iOS.

BDO's source code review started with the initialization of the SDK. The initialization of the MTGSDK object takes as input, the App ID and App Key that were generated from Mintegral's account dashboard during the registration. During the initialization of the object, the SDK collects the following information from the mobile device:

- ▶ Platform and OS version
- ▶ Application package name and version name
- ▶ Device orientation and screen size
- ▶ Device type, model, CPU type, and device uptime
- ▶ IDFA and IDFV
- ▶ Network code and Country code
- ▶ Language
- ▶ Time zone and current timestamp
- ▶ SDK version
- ▶ Battery level and charging status
- ▶ Device total and free memory sizes
- ▶ User agent
- ▶ Network type and cellular network information
- ▶ IP address
- ▶ Device name
- ▶ GPS (latitude and longitude)
- ▶ User Info including gender and age

The SDK stores the information in the local SQLite database on the device and communicates with the Mintegral API server with the information. In return, based on the device information, Mintegral API server responds with configuration information such as the number of ads to cache to optimize the ad display experience on the device. BDO reviewed a list of Mintegral server URLs embedded within the SDK and noted all using the Hypertext Transfer Protocol Secure (HTTPS) protocol for communication to ensure the information is encrypted during the transmission.

BDO noted in the source code that the **setUserInfo** method is implemented within the SDK allowing app publishers to set up user gender, age and GPS coordinates, but the method is never being called within the SDK to directly collect such information from the user. BDO also

Inquired about the purpose of setting gender and age data and the process of collecting the data. Mintegral responded that the demographic information is optional, which requires the publishers to pass the information for targeting advertisements and Mintegral does not have any way to collect user demographic information directly from the end users.

BDO further noted a method is implemented to obtain the device name which may potentially contain the full or partial name of the device user. The method returns the MD5 hash value of the actual device name and the device name hash value is included in the information transmitted for requesting ads. However, a similar property within the device information obtained by the SDK at initialization returns the un hashed actual device name, which was transmitted to the Mintegral API server.

Mintegral’s SDK offers various formats of advertisements such as banners, native ads, and videos. Depending on the types of ads, the process of displaying the ads or playing the videos may vary. In most cases, the publishers will be needed to configure and request ads in applications with a few simple settings such as dimension, position and refresh time, and additional configuration will be needed for videos such as selecting video viewer, requesting multiple ads and mute the playback. When users click on the displayed ad, the SDK captures the click event and transmits information about the displayed ad such as ad placementID, UnitID and the status of the jump to the ad URL.

The following chart illustrates the process flow and interactions between the SDK and Mintegral servers.

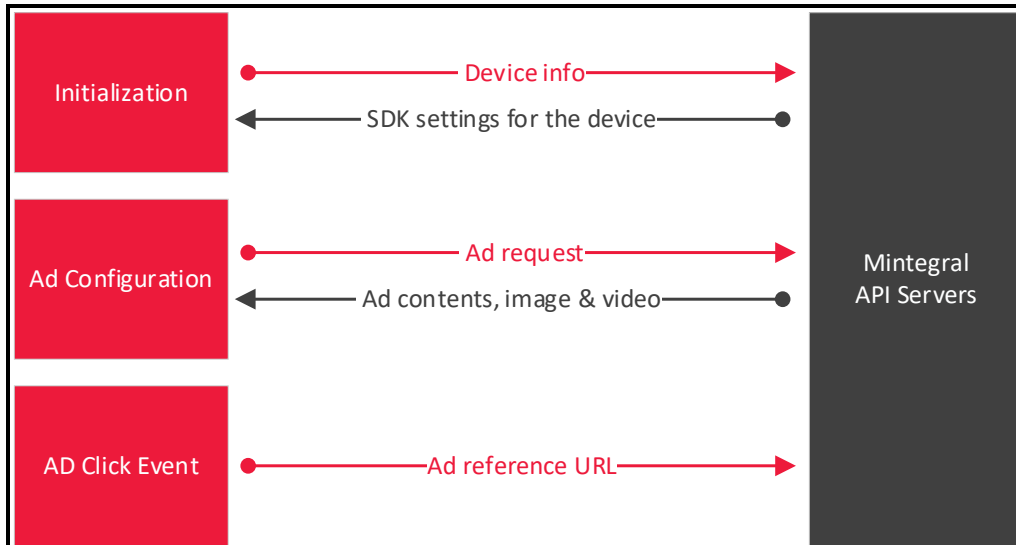


Figure 2, iOS SDK Process Flow

During the interview with the Mintegral SDK development team, BDO obtained a list of user and device information transmitted to Mintegral servers reflecting the collected data from version 6.6.5 of the iOS SDK:

Device and User Information Collected
Device type (e.g. smartphone, tablet, etc.)

Device and User Information Collected
Device model
Operating system (e.g. iOS) and the OS version of the device
Device properties related to screen size, Orientation
Battery
Carrier name
App version
Country
Language
Network connection type
IP address
Timestamp
Network status such as Wi-Fi
The identifier for advertiser (e.g. IDFA)
HTTP referrer of the ad click request
User agent
Package name
IDFV

Figure 3, Information Collected

Based on its review, BDO did not identify any Personally Identifiable Information (PII) with one exception of the information of the mobile device name, which may potentially contain the mobile device owner’s name, if so configured by the device owner.

SOURCE CODE REVIEW - ANDROID SDK

Mintegral’s open-source Android SDK version **15.1.0** contains 15 different libraries with 658² Java programming code files. The libraries are designed to provide common SDK functions, functions handling various types of advertisements, and video playback capabilities.

BDO started its review by following the process of integrating the SDK into publishers’ mobile applications. The SDK initialization takes as input, the App ID and App Key that are assigned to the publisher from Mintegral’s account registration. During the initialization, the SDK reports user and device information to Mintegral’s API server. The user information, including gender, age, and GPS (latitude, longitude) location of the device, is optional for targeting

² Note that this number (658) differs from number in the table at the beginning of this section (894) because this number only accounts for programming code files while the count of 894 includes other types of file such as configuration files (e.g. Extensible Markup Language (XML)).

user groups for custom ad experiences. The SDK collects the following information from the mobile device:

- ▶ Platform
- ▶ Device make and model, and OS version
- ▶ Google AD ID (GAID)
- ▶ Network type, Carrier ID
- ▶ Device user agent
- ▶ Screen size (width and height), resolution, and orientation
- ▶ Device country code and network code
- ▶ Language
- ▶ Package name
- ▶ System time and time zone
- ▶ Battery status and level
- ▶ Device hardware settings
- ▶ Total device memory and available memory size
- ▶ System file storage capacity and SD card status
- ▶ IP address
- ▶ Serial number
- ▶ Device user

BDO confirmed with Mintegral regarding the above list of user and device information and learned that the SDK also collects additional device information such as the International Mobile Equipment Identity (IMEI) number for users located in China. Additionally, BDO identified a function in the SDK to get the device serial number. According to Android documentation, the persistent device identifiers are protected with additional restrictions and applications require additional permissions from the user in order to access. Depending on the permissions given to the publishers' applications, the SDK may be able to access the device serial number. In addition, the SDK obtains the device's user property, which may contain Personal Identifiable Information (PII) such as the name of the device user.

After transmitting the device and user information, the SDK retrieves a set of configuration data from the Mintegral server tailored to the device for optimizing user experiences such as connection timeout period.

The SDK provides a variety of ad formats from banners to videos. The Java libraries are structured based on types of ads and related functionalities. To create the objects for specific kinds of ads, some required information such as dimensions and location for

displaying the ads will need to pass from the publishers' application to the SDK during the dynamic setup of the ad objects. When the SDK requests the contents of the ad, the data elements listed above will be transmitted to the Mintegral server along with the App ID and App Key provided by Mintegral for the publisher's account. The information is packaged and encoded using the Base64 encoding technique and is transmitted over the HTTPS protocol for data protection.

Once the requested ad is displayed on the device, an impression is reported to the Mintegral server. If the user clicks on the displayed ad, the click is reported to the server. Both events trigger the SDK to transmit the ad information such as the Unit ID of the displayed ad in addition to the device and user information mentioned above.

BDO further noticed an XML configuration file is included in the SDK for enabling the clear text traffic permission, which allows the publisher's app to utilize the unsecured HTTP protocol for transmitting data. The configuration appears to associate the permission with the device loopback IP address (127.0.0.1). According to Mintegral's SDK documentation, the configuration is needed to improve video playback performance.

Based on the review, BDO did not identify any function for specifically collecting end-user information without the user's permission. Based on Mintegral's SDK documentation, the application publishers are responsible for obtaining the end-user's consent regarding the data obtained through the SDK. BDO also found a list of the identified data elements collected by the SDK published on Mintegral's website.


BDO also noted that the SDK provides the capability to switch off the user data collection. To Comply with the European Unions' General Data Protection Regulation (GDPR), app publishers need to turn off the user data collection functions if end-user's consent is not provided.

Similarly, the SDK provides settings to satisfy the requirements for the California Consumer Privacy Act (CCPA). The app publishers can enable the **DoNotTrackStatus** property for California users, which according to the SDK documentation, Mintegral will not provide personalized ads based on the user's device information and will not share the information with its third-party partners.

Conclusions

Based on the foregoing, BDO has determined that Mintegral's control posture for Protect the Software (PS) is **ACCEPTABLE**. BDO identified that Mintegral's SDK's are not collecting and/or transmitting PII or other sensitive data and that Mintegral has endeavored to reduce the amount of data points it does collect to maintain compliance with App Store and Google Play policies.

Recommendations

 Data Collection		Device Name/User
Issue:	BDO identified that both the iOS and Android versions of Mintegral’s SDK are collecting the user’s device name (iOS = Device Name , Android = Device User).	
Why this Matters:	While not prohibited to collect by either the App Store or Google Play policy, these attributes are set by devices users and have the possibility of containing PII (e.g. Device Name = “John Smith”).	
BDO’s Recommendation:	▶ BDO recommends that Mintegral’s not collect the iOS Device Name and the Android Device User in subsequent releases of its iOS and Android SDKs.	
Update:	▶ Subsequent to completing this Assessment, BDO learned from Mobvista’s development team that these attributes had been removed from its SDK as of iOS version 6.6.8 and Android version 15.2.2 . BDO was able to verify the removal of these attributes from the indicated versions of the source code.	

PRODUCE WELL-SECURED SOFTWARE (PW)

Assessment Opinion

Practice	Assessment
PW	●

OVERVIEW

As noted in previous section, BDO obtained and reviewed a copy of Mintegral’s open-source SDK for iOS version **6.6.5** and Android version number **15.1.0**. BDO also reviewed the integration documentation provided on Mintegral’s website for assisting developers to incorporate the SDK into publishers’ mobile applications.

Based on the review of both iOS and Android versions of the Mintegral SDK, BDO identified all communications between the SDK and Mintegral’s server are transmitted through the HTTPS protocol, in which the transmission is encrypted using Transport Layer Security (TLS) or Secure Sockets Layer (SSL) to protect user data.

However, BDO noticed that the iOS SDK Integration Guide (http://cdn-adn.rayjump.com/cdn-adn/v2/markdown_v2/index.html?file=sdm_sdk-ios&lang=en) published by Mintegral instructed developers to specifically enable communication over HTTP connection to avoid the App Transport Security regulations embedded in iOS 9 or higher versions by enabling the **NSAllowsArbitraryLoads** key. BDO believes the setting allows the SDK to manually configure the server authentication methods and implement custom handling of server trust authentication. However, enabling the **NSAllowsArbitraryLoads** key may potentially expose mobile applications’ communication to the unsecured HTTP communication.

Methodology & Assessment

- ▶ Review training materials and conduct interviews to determine if there is awareness to meet security requirements for the design, development, testing, and release teams
- ▶ Review any policies related to software development to determine source code review cycles and how code is reviewed (human review vs. automation)
- ▶ Review source code to determine secure coding practices are adhered to for the language and development framework (iOS, Android)

Similarly, the Integration Guide for the Android version of the SDK (http://cdn-adn.rayjump.com/cdn-adn/v2/markdown_v2/index.html?file=sdk-m_sdk-android&lang=en) specifies the enable custom configuration to the network security settings by using a local XML file to enable the `cleartextTrafficPermitted` setting. The Android network security setup allows unsecure communication using HTTP protocol.

In addition, BDO noted that the Android SDK Integration Guide requires developers to include the `REQUEST_INSTALL_PACKAGES` permission in the Android Manifest file. This permission replaced the `INSTALLED_PACKAGES` permission which provides a blanket permission for package installation to the mobile device and it is not allowed for any third-party applications according to Google documentation. Instead, the `REQUEST_INSTALL_PACKAGES` permission prompts users to install third-party applications which is a useful security protection and enables the users to choose whether to accept the applications.

The security and quality of code in programming is important. As noted in the report, Mintegral's *Software Development Safety Management Guidelines* and *Code Security Development Management Measures* provide Mintegral development teams coding standard and definitions for consistency in code implementation. BDO's source review on both the iOS and Android versions of the SDK confirms the SDK development teams adhere to the policies.

BDO also noticed the policies emphasize security testing of software development. The policies and procedures cover from strategizing the test plan to including all data security requirements of the project; utilizing various testing techniques for a thorough coverage to uncover any potential security issues as well as the process to rectify the identified issues. BDO determined the policies and procedures are sufficient to facilitate secure software development.

App Store

BDO reviewed the policies in Apple's App Store Review Guidelines specifically related to privacy to align Mintegral's development posture to the terms set forth therein.

BDO notes that as an SDK, the Mintegral platform is not an application available for download from the App Store. Mintegral's SDK is used by application developers in their apps and it is incumbent on the app developers to comply with the App Store terms. Therefore, any in-app disclosures and authorizations for access and collection of personal and sensitive information happen at the application level, not at Mintegral's SDK level; however, where required, consent is obtained by app publishers on Mintegral's behalf and can be withdrawn by the user at any time.

BDO noted the data that can be collected by the Mintegral SDK in the previous section of this report, which aligns to the App Store's Review Guidelines Section 5.1.1 *Data Collection and Storage*:

"...(iii) Data Minimization: Apps should only request access to data relevant to the core functionality of the app and should only collect and use data that is required to accomplish the

relevant task. Where possible, use the out-of-process picker or a share sheet rather than requesting full access to protected resources like Photos or Contacts.”

Further, BDO noted previously that Mintegral is annually certified by the kidSAFE Seal Program for satisfying the requirements outlined in COPPA, which aligns with the App Store’s Review Guidelines Section 5.1.4 Kids:

“For many reasons, it is critical to use care when dealing with personal data from kids, and we encourage you to carefully review all the requirements for complying with laws like the Children’s Online Privacy Protection Act (“COPPA”), the European Union’s General Data Protection Regulation (“GDPR”), and any other applicable regulations or laws.”

Further detail may be found at:

- ▶ Mintegral: <https://www.mintegral.com/en/privacy/>
- ▶ App Store: <https://developer.apple.com/app-store/review/guidelines/#legal>

Google Play

BDO reviewed the policies in Google Play’s Policy Center Section, *Privacy, Deception and Device Abuse* to align Mintegral’s development posture to the terms set forth therein.

BDO notes that as an SDK, the Mintegral platform is not an application available for download from Google Play. Mintegral’s SDK is used by application developers in their apps and it is incumbent on the app developers to comply with Google Play’s terms. Therefore, any in-app disclosures and authorizations for access and collection of personal and sensitive information happen at the application level, not at Mintegral’s SDK level; however, where required, consent is obtained by app publishers on Mintegral’s behalf and can be withdrawn by the user at any time.

BDO noted the data that can be collected by the Mintegral SDK in the previous section of this report. Mintegral’s development team identified that this listing has been reduced from prior versions of the SDK and is in compliance with Google Play’s Policy Center Section, *Personal and Sensitive Information*:

“Personal and sensitive user data includes, but isn’t limited to, personally identifiable information, financial and payment information, authentication information, phonebook, contacts, device location, SMS and call related data, microphone, camera, and other sensitive device or usage data. If your app handles sensitive user data, then you must:

- ▶ *Limit your access, collection, use, and sharing of personal or sensitive data acquired through the app to purposes directly related to providing and improving the features of the app (e.g., user anticipated functionality that is documented and promoted in the app’s description in the Play Store)...”*


Further detail may be found at:

- ▶ Mintegral: <https://www.mintegral.com/en/privacy/>
- ▶ Google Play: <https://developer.apple.com/app-store/review/guidelines/#legal>

Conclusions

Based on the foregoing, BDO has determined that Mintegral’s control posture for Produce Well-Secured Software (PW) as **AREA FOR IMPROVEMENT**. While Mintegral’s privacy policy is in alignment to those of the App Store and Google Play, during its code review, BDO noted the potential in both the iOS and Android versions for data to be transmitted using the unsecure HTTP.

Recommendations

 Data Security HTTP	
Issue:	While all communication in the iOS and Android SDKs use HTTPS, the possibility exists in both for data to be transmitted using the unsecure HTTP as indicated in the SDK integration documentation as well as the configuration manifest in the source code.
Why this Matters:	Data transmitted via HTTP is not encrypted like HTTPS, therefore, any potentially sensitive or PII data is easily read as plain text.
BDO’s Recommendation:	▶ Disable and/or remove any classes, methods, and functions allowing use of HTTP.
Update:	Subsequent to completing this Assessment, BDO learned from Mobvista’s development team that the HTTP instructions had been removed from the SDK integration docs and configuration manifest. BDO was able to verify the removal of these attributes from the integration documentation and configuration manifest. This section was intended to explain to publishers how to adapt third party html creatives (for example creatives from other DSPs).

RESPOND TO VULNERABILITIES (RV)

Assessment Opinion

Practice	Assessment
RV	●

OVERVIEW

On September 4, 2020, Mintegral’s CEO, Erick Fang, announced on the platform’s [blog](#) that due to recent allegations its software contained vulnerabilities, it would be moving the SDK to an open source software model. This move, Fang stated, will allow for greater transparency as well as making the SDK more secure since it will be going through continual review by the open source community.

The allegations stem from an August 24, 2020 report by the security firm, Snyk, which stated that Mintegral was hijacking other applications’ ad clicks in both the iOS and Android versions of its platform.

In a subsequent vulnerability report from Snyk, the Mintegral SDK for both iOS and Android was alleged to be running the **MTGInvocationBoxing** class, which allows for remote code execution on devices where the software is installed.

In addition to moving its source repositories to an open source software model, Mintegral deleted the **MTGInvocationBoxing** class beginning with its 6.6.0.0 SDK release.

Both Apple and Google have taken steps to address this issue by placing the onus on application developers to ensure they are using the most recent versions of any third-party SDKs their applications are implementing.

Methodology & Assessment

- ▶ Review policies relative to vulnerability response
- ▶ Interview stakeholders to identify vulnerability monitoring practices (e.g. vulnerability databases, security mailing lists)
- ▶ Interview stakeholders to determine if there is a team in place to respond to identify and respond to vulnerabilities
- ▶ Interview stakeholders to determine if all source code is proactively reviewed subsequent to reported vulnerabilities to determine the vulnerability doesn’t exist in more than one place

REMEDIATION

As stated previously, Mintegral took the following steps to remediate the vulnerabilities identified by Snyk:

- ▶ Removing³ the identified vulnerabilities in its SDK
- ▶ Moved to an open source software model for its SDK by placing it in GitHub repositories accessible to registered partners

BDO has identified the following vulnerability timeline for Mintegral's remediation efforts.

³ BDO noted no classes, methods, or functions in the source code of both the iOS (6.6.5) and Android (15.1.0) versions of the source code that a) would allow remote code execution, or b) would perpetuate ad fraud.



Vulnerability Timeline

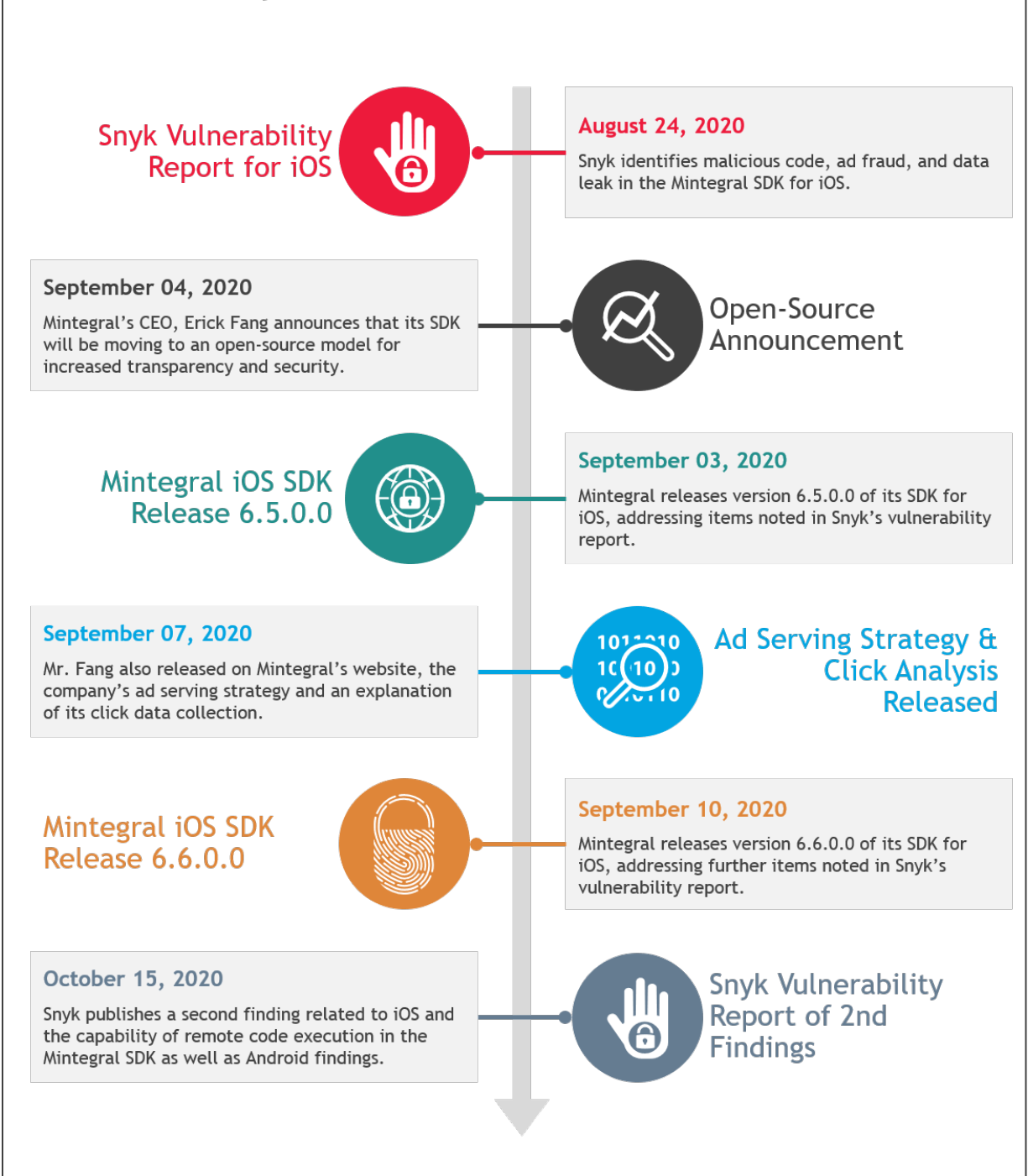


Figure 4, Vulnerability/Remediation Timeline

During its review for this Secure Software Development Assessment, BDO noticed none of the items identified in the Snyk reports existed in the iOS **6.6.5** and Android **15.1.0** versions of its SDK.

Conclusions

Based on the foregoing, BDO has determined that Mintegral's control posture for Respond to Vulnerabilities (RV) is **ACCEPTABLE**. BDO noted no instances of the potential vulnerabilities cited in the Snyk reports, therefore is under the assumption that Mintegral responded to the potential vulnerabilities identified in the Snyk reports by removing the potential vulnerabilities from its source code. Mintegral also has taken the additional step of moving the source code for its SDKs to an open source platform where it can be accessed and reviewed by registered users.