WhiteSource Audit Services

Professional Services Analysis

Date:	10/19/20
Report Provided By:	Ven Deshpande ven.deshpande@whitesourcesoftware.com

Contents:

Executive Summary:

The following is a software compositional analysis report of code various products owned by Mobvista. The goal of this audit is to analyze the given code base to determine the various sources, binaries and dependencies which compose this project. And, using WhiteSource technologies, report on the licensing requirements, security vulnerabilities and version compatibility of the open-source components in the given code. WhiteSource provides an accurate compositional analysis of the code using proprietary algorithms that suppress unnecessary information and highlight actionable data by analyzing build environments and comparing checksums. Furthermore, WhiteSource has a mature database, containing over 3 million open-source components and 70 million source files, covering more than 200 programming languages.

Analysis Summary:

This analysis was performed on libraries spread over 27 projects.

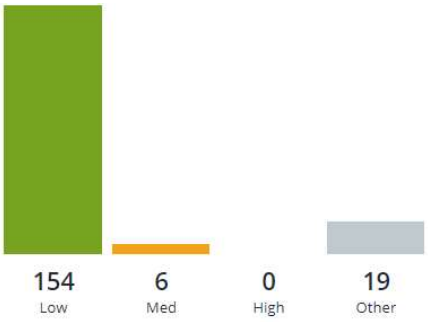
The analysis revealed the following:

- 67 alerts of various types were reported on 2699 libraries analyzed.
- One of the vulnerabilities is reported as being high risk or critical in nature.
  Note that this and other low risk vulnerabilities are distributed by Android Studio and are only on the build machine, and not within the mobile app that is run by an end user (further details in the security risk analysis section of the report).
- 15 types of open-source licenses were detected.
- No opensource libraries are reported with a high license risk score rating with the given distribution model.
- The medium risk licenses reported are not applicable the libraries flagged are unmodified.
- 54 of the analyzed libraries are outdated.
- 4 libraries have multiple versions in use.

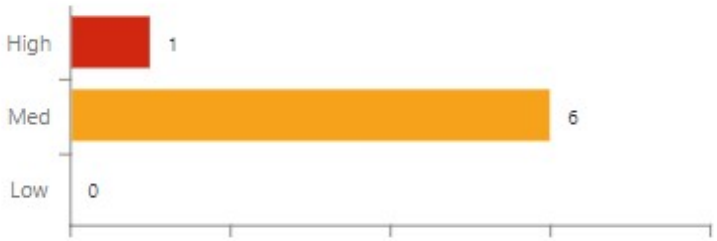
It has been indicated that these projects are distributed in a typical distribution model, in the way reciprocity is enforced by a typical copyleft license.

Analysis Dashboard:

The following charts describe the overall risk disposition of the entire codebase:



License risk distribution chart



Vulnerability Severity distribution chart

Overview of Risk by Products:

The following table describes the risk distribution per project.

Product/Project	Libraries	Licenses	Security & Quality
Mobvista_Android	Total: 2, Direct: 2, Dependencies: 0	Total 2	No Security Vulnerabilities
		No Risky Licenses	No Outdated Libraries
mtgbid	Total: 111, Direct: 38, Dependencies: 73	Total 11	4 Security Vulnerabilities
		Higher Risks: LGPL 2.1 (1), Eclipse 1.0 (1)	28 Outdated Libraries

Product/Project	Libraries	Licenses	Security & Quality
mtgbanner	Total: 115, Direct: 39, Dependencies: 76	Total 11	4 Security Vulnerabilities
		Higher Risks: LGPL 2.1 (1), Eclipse 1.0 (4)	29 Outdated Libraries
nativeex	Total: 115, Direct: 39, Dependencies: 76	Total 11	4 Security Vulnerabilities
		Higher Risks: LGPL 2.1 (1), Eclipse 1.0 (4)	29 Outdated Libraries
videojs	Total: 115, Direct: 39, Dependencies: 76	Total 11	4 Security Vulnerabilities
		Higher Risks: LGPL 2.1 (1), Eclipse 1.0 (4)	29 Outdated Libraries
mtgjscommon	Total: 115, Direct: 40, Dependencies: 75	Total 11	4 Security Vulnerabilities
		Higher Risks: LGPL 2.1 (1), Eclipse 1.0 (4)	29 Outdated Libraries

Product/Project	Libraries	Licenses	Security & Quality
optimizedata	Total: 75, Direct: 3, Dependencies: 72	Total 9	5 Security Vulnerabilities
		Higher Risks: LGPL 2.1 (1), Eclipse 1.0 (1)	2 Outdated Libraries
mtgdownloads	Total: 111, Direct: 38, Dependencies: 73	Total 11	4 Security Vulnerabilities
		Higher Risks: LGPL 2.1 (1), Eclipse 1.0 (1)	28 Outdated Libraries
chinacommon	Total: 73, Direct: 1, Dependencies: 72	Total 8	4 Security Vulnerabilities
		Higher Risks: LGPL 2.1 (1)	1 Outdated Libraries
mtgsplash	Total: 130, Direct: 56, Dependencies: 74	Total 11	5 Security Vulnerabilities
		Higher Risks: LGPL 2.1 (1), Eclipse 1.0 (5)	41 Outdated Libraries
aarlib	Total: 115, Direct: 43, Dependencies: 72	Total 11	4 Security Vulnerabilities
		Higher Risks: LGPL 2.1 (1)	28 Outdated Libraries

Product/Project	Libraries	Licenses	Security & Quality
playercommon	Total: 115, Direct: 40, Dependencies: 75	Total 11	4 Security Vulnerabilities
		Higher Risks: LGPL 2.1 (1), Eclipse 1.0 (4)	29 Outdated Libraries
app	Total: 136, Direct: 59, Dependencies: 77	Total 12	6 Security Vulnerabilities
		Higher Risks: LGPL 2.1 (1), Eclipse 1.0 (4)	37 Outdated Libraries
interactiveads	Total: 115, Direct: 39, Dependencies: 76	Total 11	4 Security Vulnerabilities
		Higher Risks: LGPL 2.1 (1), Eclipse 1.0 (4)	29 Outdated Libraries
interstitialvideo	Total: 112, Direct: 39, Dependencies: 73	Total 11	4 Security Vulnerabilities
		Higher Risks: LGPL 2.1 (1), Eclipse 1.0 (1)	28 Outdated Libraries

Product/Project	Libraries	Licenses	Security & Quality
appwallext	Total: 115, Direct: 39, Dependencies: 76	Total 11	4 Security Vulnerabilities
		Higher Risks: LGPL 2.1 (1), Eclipse 1.0 (4)	29 Outdated Libraries
buildtask	Total: 83, Direct: 11, Dependencies: 72	Total 11	4 Security Vulnerabilities
		Higher Risks: LGPL 2.1 (1)	2 Outdated Libraries
alphab	Total: 115, Direct: 40, Dependencies: 75	Total 11	4 Security Vulnerabilities
		Higher Risks: LGPL 2.1 (1), Eclipse 1.0 (4)	29 Outdated Libraries
mtgnative	Total: 115, Direct: 39, Dependencies: 76	Total 11	4 Security Vulnerabilities
		Higher Risks: LGPL 2.1 (1), Eclipse 1.0 (4)	29 Outdated Libraries
common	Total: 117, Direct: 42, Dependencies: 75	Total 11	4 Security Vulnerabilities

Product/Project	Libraries	Licenses	Security & Quality
		Higher Risks: LGPL 2.1 (1), Eclipse 1.0 (4)	29 Outdated Libraries
interstitial	Total: 115, Direct: 39, Dependencies: 76	Total 11	4 Security Vulnerabilities
		Higher Risks: LGPL 2.1 (1), Eclipse 1.0 (4)	29 Outdated Libraries
appwall	Total: 115, Direct: 40, Dependencies: 75	Total 11	4 Security Vulnerabilities
		Higher Risks: LGPL 2.1 (1), Eclipse 1.0 (4)	29 Outdated Libraries
mtgnativeadvanced	Total: 130, Direct: 56, Dependencies: 74	Total 11	5 Security Vulnerabilities
		Higher Risks: LGPL 2.1 (1), Eclipse 1.0 (5)	41 Outdated Libraries
videocommon	Total: 115, Direct: 39, Dependencies: 76	Total 11	4 Security Vulnerabilities
		Higher Risks: LGPL 2.1 (1), Eclipse 1.0 (4)	29 Outdated Libraries

Product/Project	Libraries	Licenses	Security & Quality
reward	Total: 116, Direct: 40, Dependencies: 76	Total 11	4 Security Vulnerabilities
		Higher Risks: LGPL 2.1 (1), Eclipse 1.0 (4)	29 Outdated Libraries
Mobvista_IOS	Total: 0, Direct: 0, Dependencies: 0	Total 0	No Security Vulnerabilities
		No Risky Licenses	No Outdated Libraries
MTGSDK	Total: 8, Direct: 2, Dependencies: 6	Total 2	No Security Vulnerabilities
		No Risky Licenses	2 Outdated Libraries

Analysis Methodology Overview:

The analysis involves initiating a scan by configuring the White Source Unified Agent with the projects' environment variables. During this process, WhiteSource generates SHA-1 files for every scanned file and matches them against a knowledge base of opensource projects. Dependencies are calculated based on the build environment. Once a match is established, additional data from the knowledgebase about the library is applied to the project. Simultaneously, various security vulnerabilities (CVE) reported for the libraries are also retrieved. In addition, other properties such as severity level, date of publishing, description are also reported on. After the analysis is completed, an inventory of the project is generated, and various risk rate scorings are calculated.

In the WhiteSource environment, all opensource licenses are assigned a risk score rating based on the various obligations that the license enforces. Licensing experts at WhiteSource have analyzed various opensource licenses and attributed a risk score, while considering various factors such as copyright, patent and royalty risk, reciprocity, linking etc. Components that have a high-risk rating typically are considering to be incompatible with a commercial license and

require a review. These libraries would usually cause the derived work to be licensed under an open-source license, if used improperly. Reciprocal licenses such as GPL, LGPL, AGPL etc. are considered to have a high-risk score rating based their copyleft risk score setting.

License Risk Analysis Overview:

The analysis revealed that the code base uses 7 types of open-source licenses.

About half of detected components are from low-risk licenses. However, the other components originate from restrictive licenses.

Note that the distribution model of the product effects the obligations of open-source licenses.

The overall distribution of these is displayed in the following sections.

High License Risk Libraries:

The following chart describes the components with a high-risk score:

License	Library	Project
N/A	None	N/A

Components with Medium License Risk:

License	Library	Project	Note
Eclipse 1.0	org.jacoco.ant-0.7.9.jar	mtgsplash	1
Eclipse 1.0	org.jacoco.ant-0.7.9.jar	nativeex	
Eclipse 1.0	org.jacoco.ant-0.7.9.jar	mtgbanner	
Eclipse 1.0	org.jacoco.ant-0.7.9.jar	mtgjscommon	
Eclipse 1.0	org.jacoco.ant-0.7.9.jar	videojs	
Eclipse 1.0	org.jacoco.ant-0.7.9.jar	appwallext	
Eclipse 1.0	org.jacoco.ant-0.7.9.jar	alphab	
Eclipse 1.0	org.jacoco.ant-0.7.9.jar	playercommon	
Eclipse 1.0	org.jacoco.ant-0.7.9.jar	interactiveads	
Eclipse 1.0	org.jacoco.ant-0.7.9.jar	app	
Eclipse 1.0	org.jacoco.ant-0.7.9.jar	videocommon	
Eclipse 1.0	org.jacoco.ant-0.7.9.jar	mtgnativeadvanced	
Eclipse 1.0	org.jacoco.ant-0.7.9.jar	reward	
Eclipse 1.0	org.jacoco.ant-0.7.9.jar	common	
Eclipse 1.0	org.jacoco.ant-0.7.9.jar	mtgnative	
Eclipse 1.0	org.jacoco.ant-0.7.9.jar	appwall	
Eclipse 1.0	org.jacoco.ant-0.7.9.jar	interstitial	
Eclipse 1.0	org.jacoco.agent-0.7.9.jar	mtgdownloads	
Eclipse 1.0	org.jacoco.agent-0.7.9.jar	mtgsplash	
Eclipse 1.0	org.jacoco.agent-0.7.9.jar	nativeex	
Eclipse 1.0	org.jacoco.agent-0.7.9.jar	mtgbanner	

License	Library	Project	Note
Eclipse 1.0	org.jacoco.agent-0.7.9.jar	mtgjscommon	
Eclipse 1.0	org.jacoco.agent-0.7.9.jar	videojs	
Eclipse 1.0	org.jacoco.agent-0.7.9.jar	appwallext	1
Eclipse 1.0	org.jacoco.agent-0.7.9.jar	interstitialvideo	
Eclipse 1.0	org.jacoco.agent-0.7.9.jar	alphab	
Eclipse 1.0	org.jacoco.agent-0.7.9.jar	playercommon	
Eclipse 1.0	org.jacoco.agent-0.7.9.jar	interactiveads	
Eclipse 1.0	org.jacoco.agent-0.7.9.jar	app	
Eclipse 1.0	org.jacoco.agent-0.7.9.jar	videocommon	
Eclipse 1.0	org.jacoco.agent-0.7.9.jar	mtgnativeadvanced	
Eclipse 1.0	org.jacoco.agent-0.7.9.jar	reward	
Eclipse 1.0	org.jacoco.agent-0.7.9.jar	common	
Eclipse 1.0	org.jacoco.agent-0.7.9.jar	mtgnative	
Eclipse 1.0	org.jacoco.agent-0.7.9.jar	appwall	
Eclipse 1.0	org.jacoco.agent-0.7.9.jar	interstitial	
Eclipse 1.0	org.jacoco.agent-0.7.9.jar	mtgbid	
Eclipse 1.0	org.jacoco.report-0.7.9.jar	mtgsplash	
Eclipse 1.0	org.jacoco.report-0.7.9.jar	nativeex	
Eclipse 1.0	org.jacoco.report-0.7.9.jar	mtgbanner	
Eclipse 1.0	org.jacoco.report-0.7.9.jar	mtgjscommon	
Eclipse 1.0	org.jacoco.report-0.7.9.jar	videojs	
Eclipse 1.0	org.jacoco.report-0.7.9.jar	appwallext	
Eclipse 1.0	org.jacoco.report-0.7.9.jar	alphab	
Eclipse 1.0	org.jacoco.report-0.7.9.jar	playercommon	
Eclipse 1.0	org.jacoco.report-0.7.9.jar	interactiveads	
Eclipse 1.0	org.jacoco.report-0.7.9.jar	app	
Eclipse 1.0	org.jacoco.report-0.7.9.jar	videocommon	
Eclipse 1.0	org.jacoco.report-0.7.9.jar	mtgnativeadvanced	
Eclipse 1.0	org.jacoco.report-0.7.9.jar	reward	
Eclipse 1.0	org.jacoco.report-0.7.9.jar	common	
Eclipse 1.0	org.jacoco.report-0.7.9.jar	mtgnative	
Eclipse 1.0	org.jacoco.report-0.7.9.jar	appwall	
Eclipse 1.0	org.jacoco.report-0.7.9.jar	interstitial	
Eclipse 1.0	org.jacoco.core-0.7.9.jar	mtgsplash	
Eclipse 1.0	org.jacoco.core-0.7.9.jar	nativeex	
Eclipse 1.0	org.jacoco.core-0.7.9.jar	mtgbanner	
Eclipse 1.0	org.jacoco.core-0.7.9.jar	mtgjscommon	
Eclipse 1.0	org.jacoco.core-0.7.9.jar	videojs	
Eclipse 1.0	org.jacoco.core-0.7.9.jar	appwallext	
Eclipse 1.0	org.jacoco.core-0.7.9.jar	alphab	
Eclipse 1.0	org.jacoco.core-0.7.9.jar	playercommon	
Eclipse 1.0	org.jacoco.core-0.7.9.jar	interactiveads	

License	Library	Project	Note
Eclipse 1.0	org.jacoco.core-0.7.9.jar	app	
Eclipse 1.0	org.jacoco.core-0.7.9.jar	videocommon	
Eclipse 1.0	org.jacoco.core-0.7.9.jar	mtgnativeadvanced	
Eclipse 1.0	org.jacoco.core-0.7.9.jar	reward	
Eclipse 1.0	org.jacoco.core-0.7.9.jar	common	
Eclipse 1.0	org.jacoco.core-0.7.9.jar	mtgnative	
Eclipse 1.0	org.jacoco.core-0.7.9.jar	appwall	
Eclipse 1.0	org.jacoco.core-0.7.9.jar	interstitial	
Eclipse 1.0	junit-4.12.jar	optimizedata	
Eclipse 1.0	junit-4.12.jar	mtgnativeadvanced	
Eclipse 1.0	junit-4.12.jar	mtgsplash	
LGPL 2.1	trove4j-20160824.jar	mtgdownloads	2
LGPL 2.1	trove4j-20160824.jar	optimizedata	
LGPL 2.1	trove4j-20160824.jar	mtgsplash	
LGPL 2.1	trove4j-20160824.jar	chinacommon	
LGPL 2.1	trove4j-20160824.jar	nativeex	
LGPL 2.1	trove4j-20160824.jar	mtgbanner	
LGPL 2.1	trove4j-20160824.jar	mtgjscommon	
LGPL 2.1	trove4j-20160824.jar	videojs	
LGPL 2.1	trove4j-20160824.jar	appwallext	
LGPL 2.1	trove4j-20160824.jar	interstitialvideo	
LGPL 2.1	trove4j-20160824.jar	alphab	
LGPL 2.1	trove4j-20160824.jar	buildtask	
LGPL 2.1	trove4j-20160824.jar	playercommon	
LGPL 2.1	trove4j-20160824.jar	aarlib	
LGPL 2.1	trove4j-20160824.jar	interactiveads	
LGPL 2.1	trove4j-20160824.jar	app	
LGPL 2.1	trove4j-20160824.jar	videocommon	
LGPL 2.1	trove4j-20160824.jar	mtgnativeadvanced	
LGPL 2.1	trove4j-20160824.jar	reward	
LGPL 2.1	trove4j-20160824.jar	common	
LGPL 2.1	trove4j-20160824.jar	mtgnative	
LGPL 2.1	trove4j-20160824.jar	appwall	
LGPL 2.1	trove4j-20160824.jar	interstitial	

Medium License Risk notes:

1	Analysis detected various occurrences of two libraries in the analyzed code base that are licensed under the Eclipse License 1.0. This license has a partial copyleft risk that makes any modifications made to the libraries to be shared under the same license. Unmodified redistribution, however, is allowed under any license. The usage of these libraries needs

	to be reviewed. Also, this obligation is applicable to only those products that are “shipped” to end users. SaaS applications are exempt from this. Since the matches flagged are based on a checksum match, it can be assumed that these distributions are unmodified, hence these risks are not applicable.
2	Occurrences of a single library that is licensed under the LGPL license was detected in the audit. The LGPL license has a partial copyleft risk that makes any modifications made to this library to be redistributed under the same license. Dynamic linking to these libraries and unmodified redistributions are allowed for commercial licensing. Since the matches flagged are based on a checksum match, it can be assumed that these distributions are unmodified, hence these risks are not applicable Also, this obligation is applicable only to those products that are “shipped” to end users. SaaS applications are exempt from this.

Security Risk Analysis Overview:

The Common Vulnerability Scoring System (CVSS) is a free and open industry standard for assessing the severity of computer system security vulnerabilities. Based on the value of the base score range various severity levels are assigned. CVSS v2.0 assigns three severity levels of High, Medium, Low and CVSS v3.0 has five severity levels. Those vulnerabilities that are published by Mitre and NVD have a CVE prefix in their vulnerability ID. In addition to tracking such reported vulnerabilities, WhiteSource additionally provides alerts on vulnerabilities reported by scanning other repositories and advisories such as Bugzilla, GitHub issue tracker, Node Security etc. These are presented with a ws prefix in their vulnerability ID.

The following table presents the various vulnerabilities that were reported with a high severity setting. For a complete list of the vulnerabilities, see the report appendix B.

Severity	Library	Vulnerability ID	Project
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000180	aarlib
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000180	alphab
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000180	app
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000180	appwall
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000180	appwallext
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000180	buildtask
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000180	chinacommon
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000180	common
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000180	interactiveads
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000180	interstitial
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000180	interstitialvideo
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000180	mtgbanner
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000180	mtgbid
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000180	mtgdownloads
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000180	mtgjscommon

Severity	Library	Vulnerability ID	Project
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000180	mtgnative
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000180	mtgnativeadvanced
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000180	mtgsplash
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000180	nativeex
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000180	optimizedata
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000180	playercommon
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000180	reward
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000180	videocommon
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000180	videojs
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000613	aarlib
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000613	alphab
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000613	app
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000613	appwall
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000613	appwallext
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000613	buildtask
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000613	chinacommon
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000613	common
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000613	interactiveads
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000613	interstitial
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000613	interstitialvideo
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000613	mtgbanner
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000613	mtgbid
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000613	mtgdownloads
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000613	mtgjscommon
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000613	mtgnative
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000613	mtgnativeadvanced
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000613	mtgsplash
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000613	nativeex
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000613	optimizedata
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000613	playercommon
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000613	reward
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000613	videocommon
High	bcprov-jdk15on-1.56.jar	CVE-2018-1000613	videojs
High	bcprov-jdk15on-1.56.jar	CVE-2019-17359	aarlib
High	bcprov-jdk15on-1.56.jar	CVE-2019-17359	alphab
High	bcprov-jdk15on-1.56.jar	CVE-2019-17359	app
High	bcprov-jdk15on-1.56.jar	CVE-2019-17359	appwall
High	bcprov-jdk15on-1.56.jar	CVE-2019-17359	appwallext
High	bcprov-jdk15on-1.56.jar	CVE-2019-17359	buildtask
High	bcprov-jdk15on-1.56.jar	CVE-2019-17359	chinacommon
High	bcprov-jdk15on-1.56.jar	CVE-2019-17359	common
High	bcprov-jdk15on-1.56.jar	CVE-2019-17359	interactiveads

Severity	Library	Vulnerability ID	Project
High	bcprov-jdk15on-1.56.jar	CVE-2019-17359	interstitial
High	bcprov-jdk15on-1.56.jar	CVE-2019-17359	interstitialvideo
High	bcprov-jdk15on-1.56.jar	CVE-2019-17359	mtgbanner
High	bcprov-jdk15on-1.56.jar	CVE-2019-17359	mtgbid
High	bcprov-jdk15on-1.56.jar	CVE-2019-17359	mtgdownloads
High	bcprov-jdk15on-1.56.jar	CVE-2019-17359	mtgjscommon
High	bcprov-jdk15on-1.56.jar	CVE-2019-17359	mtgnative
High	bcprov-jdk15on-1.56.jar	CVE-2019-17359	mtgnativeadvanced
High	bcprov-jdk15on-1.56.jar	CVE-2019-17359	mtgsplash
High	bcprov-jdk15on-1.56.jar	CVE-2019-17359	nativeex
High	bcprov-jdk15on-1.56.jar	CVE-2019-17359	optimizedata
High	bcprov-jdk15on-1.56.jar	CVE-2019-17359	playercommon
High	bcprov-jdk15on-1.56.jar	CVE-2019-17359	reward
High	bcprov-jdk15on-1.56.jar	CVE-2019-17359	videocommon
High	bcprov-jdk15on-1.56.jar	CVE-2019-17359	videojs

Note on High Severity Vulnerabilities:

The audit revealed High Severity vulnerabilities reported on the library **bcprov-jdk15on-1.56.jar,** and other lower risk vulnerabilities in several other libraries detailed in appendix B. Further research indicates that all of these libraries are included as a part of Google Android build system. With regards to remediating this, if Google does not update that dependency, there is not much that can be done. Whilst the reported vulnerabilities are marked as critical, it is less of a concern regarding the audited app here, because the file is used by the build tools and not by the application.

Compatibility Risk Overview:

Analysis detected 54 outdated libraries in the codebase. These range from 21 libraries that are outdated by a single version, 14 by 2 versions, and 19 by over 3 versions. A detailed list of these libraries and suggested remediation efforts are listed in Appendix D of this report.

There are indications of 4 libraries that have multiple versions included in the code base.

This only analyzes multi-version usage within the same product, not multi-version libraries throughout the organization (i.e. using different versions of a library in two separate deliverable products does not count as multi-version usage).

Audit Report Overview:

This report contains the following additional sections:

Appendix A: Due Diligence Report.

This report provides a bill of materials that lists the various libraries that were detected in the analysis. Additional information such as licenses, risk score, copyright and references to the home of the library can also be found in this report.

Appendix B: Security Vulnerabilities Report

This report provides a list of all the vulnerabilities that have been generated for this project.

Appendix C: License Text and Attributions Report

This list provides a list of various licenses for this project and their license texts.

Appendix D: Compatibility Risk Report.

This report provides a list of outdated and multi-versioned libraries and suggested remediation actions.