APPVISORY PrePentest

Kicktipp (iOS)

Durchschnitt CVSS* 0.0 (low)

Höchster CVSS* 0.0 (low)

App-Informationen

• Hersteller	Kicktipp GmbH
• Name	Kicktipp
• Betriebssystem	iOS
• Version	4.11.6
• Erscheinungsdatum	16.01.2024
• BundleIdentifier	com.kicktipp.kicktippiphone
• Benötigte OS-Version	15.0
• Store-Link	https://apps.apple.com/us/app/kicktipp/id570703120
• Store-Kategorie	Sport

* CVSS Calculator: https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator

Inhaltsverzeichnis

1 Übersicht

Kicktipp	Version 4.11.6	iOS
Datenschutzverstöße • kein Verstoß festgestellt.		
	Einstufung	**unbedenklich**
Datensicherheitsverstöße • kein Verstoß festgestellt.		
	Einstufung	**unbedenklich**
Datenschutzerklärung • Das Modul wurde nicht gebucht.		
	Einstufung	**nicht verfügbar**
SSL/TLS Analyse[i] • eine Man-In-The-Middle-Attacke war nicht erfolgreich. CVSS: 0		
	Einstufung	**unbedenklich**

1.1 Zusammenfassung

Die Nutzung von externen Trackern oder Analyse-Tools konnte festgestellt werden. Es werden Daten nur verschlüsselt an den Hersteller gesendet. Die App ist voll von Werbung.

2 Zusätzliche Funktionalitäten[ii]

2.1 In-App-Käufe

In der Applikation sind keine In-App-Käufe möglich.

2.2 Externe Cloud-Dienste

Es sind Cloud-Dienste eingebunden.

2.3 Externe Login-Dienste

Die Applikation ermöglicht keinen verkürzten Registrierungs- und Loginprozess über externe Login-Dienste.

2.4 Social Network Sharing

Die App ermöglicht kein Sharing von Inhalten und Nutzerkommentaren über soziale Netzwerke.

2.5 Verwendung Webviews

Die Applikation verwendet Webviews.

3 Durchgeführte Analysevektoren

TLS analysierbar	**Ja**

Sniffing Item	Kategorie	Übertragung festgestellt	Verschlüsselung
Login-Daten	Personal Data	**Ja**	**Ja**

Hinweis: Grundsätzlich wird empfohlen, die Kommunikation zwischen Applikation und Servern ausschließlich über verschlüsselte Verbindungen vorzunehmen.

4 Testergebnisse[iii]

4.1 Test Setup[iv]

- Testdatum 27. Mai 2024
- Testgerät iPad Pro (iOS 16.3)
- Testumgebung mediaTest digital Testlabor
- Prüfspezifikation mediaTest digital Prüfspezifikation rev. 2.4

4.2 Drittanbieter-Module[v]

Die Untersuchung des von der Applikation erzeugten Datenverkehrs während des Testlaufs sowie einer statischen Analyse zeigt die Einbindung folgender externer Dienste.

Modul	Beschreibung
• Google Doubleclick	Analytics, Profiling
• Google Ads	Analytics, Profiling
• admob	Analytics, Profiling

4.3 Virenanalyse[vi]

• Dateiname	com.kicktipp.kicktippiphone-4.11.6.ipa
• SHA256 Hashwert	890e5ff75ddf07db4b567580f23c15290c3e70925285a7c75bdc4c5daadd8cdf
• Virenscan-Ergebnis	**Funde: 0 von 66**

4.4 Berechtigungsanalyse[vii]

Die Applikation fordert die folgenden Berechtigungen an.

Berechtigung	Beschreibung	Einstufung	Nutzung	Notwendig
• Kamera	Erlaubt einer App den Zugriff auf die Kamera.	• riskant	Ja	Ja

Die Berechtigungsanalyse zeigt die Verwendung von **1 Berechtigungen**, die zur Verwendung aller Funktionen der Applikation benötigt werden. Die Applikation ruft **nur die Berechtigungen ab**, die für den Funktionsumfang notwendig sind. Die Applikation wird als **nicht überprivilegiert eingestuft.**

4.5 Binärdatei-Analyse[viii]

Problematik	Schweregrad	Standards	Beschreibung
-	-	-	-

4.6 Risikobewertung[ix]

4.6.1 Datenschutzverstöße[x]

Keine Funde festgestellt	siehe **-** / **-**
Handlungsempfehlung: Kein Handlungsbedarf	

4.6.2 Datensicherheitsverstöße[xi]

Keine Funde festgestellt	siehe **-** / **-**
Handlungsempfehlung: Kein Handlungsbedarf	
HINWEIS:	
Handlungsempfehlung: Kein Handlungsbedarf	

5 Verbindungsanalyse[xii]

5.1 Analyse Serververbindungen

Nr.	Servername	IP-Adresse	Port	Land	Betreiber-	Quelle
V1	.app-measurement.com	142.250.185.142	443	US	Google Ads	Dynamische Analyse
V2	googleads.g.doubleclick-cn.net	172.217.16.194	443	US	Google Doubleclick	Dynamische Analyse
V3	admob-gmats.uc.r.appspot.com	142.250.185.212	443	US	Datadog	Dynamische Analyse
V4	www.kicktipp.de	178.63.143.193	443	DE	Kicktipp	Dynamische Analyse

5.1.1 Auszug Datenübertragungsprotokoll[xiii]

Nichts anzuzeigen

6 Entwicklerinformationen[xiv]

7 Mitigationstechniken[xv]

Position-independent-Executable	**Enabled**
Automatic-Reference-Counting	**Enabled**
Stack-Canary	**Enabled**

i Komplexität des MitM-Angriffs

Wir unterteilen die Komplexität des Man in the Middle (MitM)-Angriffs in drei Stufen. Diese ermöglichen eine einfache Einschätzung des Angriffsvektors beim Kunden.

- Verstoß – es wurden keine effektiven Gegenmaßnahmen identifiziert
- bedenklich – es wurden rudimentäre Gegenmaßnahmen identifiziert
- unbedenklich – es wurden effektive Gegenmaßnahmen identifiziert
- nicht verfügbar – die Gegenmaßnahmen machten einen MitM-Angriff nicht durchführbar

Hinweis: Grundsätzlich wird empfohlen, die Kommunikation zwischen Applikation und Servern ausschließlich über verschlüsselte Verbindungen vorzunehmen.

ii Zusätzliche Funktionalitäten

Mobile Applikationen können über Drittanbieter erweiterte Funktionalitäten bieten. Dabei umfasst die Bandbreite neben In-App-Käufen zur Funktionserweiterung oder Entfernung von Werbung auch die externe Speicherung von Nutzerdaten in Cloud-Speicherdiensten, das Teilen von Meldungen über soziale Netzwerke oder die Registrierung eines Nutzeraccounts über ein bereits bestehendes Profil eines sozialen Netzwerks.

iii Testergebnisse

In diesem Kapitel sind die Ergebnisse des Application Security Audits zusammengefasst. Das zugrunde liegende Testverfahren kann in der aktuell gültigen mediaTest digital Prüfspezifikation [separate Anlage] nachgelesen werden. Getestet wurde im Testlabor der mediaTest digital GmbH.

Das Testverfahren beinhaltet keine Aussagen über Funktionalität und Design sowie Performance und Stabilität der getesteten Applikation. Aussagen über Sicherheitslücken in angeschlossenen Backend-Systemen können lediglich in geringem Umfang getroffen werden.

Die vollständige Verbindungsanalyse kann im Kapitel 5 des Testberichtes eingesehen werden. Dort finden sich ausführliche Informationen über Datenverbindungen und Datentransfer.

iv Test Setup

Der Testdurchlauf wurde im Testlabor der mediaTest digital GmbH durch einen Application Security Analyst durchgeführt. Getestet wurde auf einem physischem Testgerät.
Grundsätzlich ist sowohl ein hoher Verbreitungsgrad des Testgerätes ebenso gegeben wie die Verwendung einer gängigen Version des Betriebssystems.

v Drittanbieter-Module

Während des Testlaufs wurde die Applikation hinsichtlich eingebundener Module und Bibliotheken von Drittanbietern untersucht. Diese Module bieten erweiterte Funktionalitäten (z.B. durch die Bereitstellung von Kartenmaterial), erlauben die Auslieferung von Werbung oder erheben

Nutzerstatistiken.

vi Virenanalyse

Während der Virenanalyse über die virustotal API durchläuft die Applikationsdatei über 50 Virenscanner. So kann eine, je nach Ergebnis gewichtete Aussage, über eine potenzielle Bedrohung durch Viren oder Trojaner getroffen werden.

vii Berechtigungsanalyse

Die Berechtigungsanalyse basiert auf einer statischen Analyse während des Testlaufs. Aufgerufene Berechtigungen werden – soweit möglich – dynamisch durch einen Application Security Analyst verifiziert. Schlägt eine manuelle Verifizierung fehl, wird die Berechtigung als „potenziell genutzt“ eingestuft.

Berechtigungen werden in mehrere Schweregrade eingestuft, die sich am Zugriff der Applikation auf Nutzerdaten orientieren:

• system Höchstes Risiko.

Die Applikation muss mit dem identischen Zertifikat signiert sein wie die Applikationen auf Betriebssystemebene. Bei Aufruf der Berechtigung durch die Applikation wird der Nutzer **nicht** nach seiner Zustimmung gefragt.

• riskant Hohes Risiko.

Die Applikation erhält Zugriff auf Nutzerdaten oder weitreichende Funktionalitäten des Betriebssystems. Bei Aufruf der Berechtigung durch die Applikation wird der Nutzer nach seiner Zustimmung gefragt.

• normal Niedriges Risiko.

Die Applikation erhält isolierten Zugriff auf Applikationsebene und kann nicht auf Nutzerdaten oder weitreichende Funktionalitäten des Betriebssystems zugreifen. Bei Aufruf der Berechtigung durch die Applikation wird der Nutzer nach seiner Zustimmung gefragt.

• selbst erstellt

Durch den Entwickler selbst erstellte Berechtigung. Diese dient der Funktionalität der Applikation und erlaubt keinen Zugriff auf Nutzerdaten oder weitreichende Funktionalitäten des Betriebssystems.

viii **Binärdatei-Analyse**

In der Binärdatei-Analyse werden erste Anzeichen von möglichen Schwachstellen aufgezeigt. Diese sind aber immer im Kontext zu betrachten, und werden dann explizit in der Zusammenfassung erläutert.

ix **Risikobewertung**

Anhand des aufgezeichneten Datenverkehrs während des Testlaufs sowie auf Basis einer statischen Analyse werden Sicherheitslücken und damit potentielle Risiken überprüft, die mit der Nutzung der Applikation einhergehen können.

Die Auswertung des Testlaufs erfolgt halb-automatisiert und wird durch einen Application Security Analyst vorgenommen. Im Zuge einer Kernfunktionalitäts- und Plausibilitätsprüfung wurde dabei besonderer Wert auf Datenübermittlungen und Berechtigungen gelegt, die zur Ausführung der primären Funktionen der Applikation nicht unbedingt notwendig sind oder für den Nutzer keinen Mehrwert bieten.

Weiterführende Details zu während des Testlaufs festgestellten Datenschutz- und Datensicherheitsverstößen werden im Kapitel 4 in der Datenübertragungsanalyse aufgelistet. Die Handlungsempfehlungen bieten für den Entwickler der Applikation eine erste Hilfestellung, identifizierte Probleme zu beheben.

x **Datenschutzverstöße**

In diesem Unterkapitel werden die Datenschutzverstöße aufgelistet und eine Handlungsempfehlung abgegeben. Als Datenschutzverstoß wird die Übertragung eines personenbezogenen oder anderweitig sensiblen Datums an Dritte definiert.

xi **Datensicherheitsverstößen**

In diesem Unterkapitel werden die Datensicherheitsverstöße aufgelistet und eine Handlungsempfehlung abgegeben. Als Datensicherheitsverstoß wird die Übertragung von Daten über eine unverschlüsselte Verbindung definiert.

xii **Verbindungsanalyse**

In diesem Kapitel werden ausführliche Informationen über die während des Testlaufs aufgezeichneten Datenübertragungen bereitgestellt.

In diesem Unterkapitel werden die Server aufgelistet, zu denen die Applikation während des Testlaufs Verbindungen aufgebaut hat.

xiii **Auszug Datenübertragungsprotokoll**

xiv **Entwicklerinformationen**

C-Based Toolchain Hardening sind Techniken um sicheren und zuverlässigen Code zu garantieren und bei dem kompilieren des Programmcodes helfen, bestimme Fehlerquellen in den Programmiersprachen Objective-C und Swift zu verhindern.

Position-independent-Executable (PIE): Eine Position-independent-Executable kann an einer beliebigen Stelle im Speicher ausgeführt werden, ohne diese vorher zu modifizieren. Dies unterscheidet sich vom absoluten Code, welcher an einem bestimmten Ort geladen werden muss, um ordnungsgemäß zu funktionieren und load-time locatable Code der von einem Linker oder Program-loader vor der Ausführung modifiziert werden muss, so dass er von einer bestimmten Adresse im Speicher ausgeführt werden kann.

Automatic-Reference-Counting (ARC): Unter Reference Counting versteht man in der Programmierung eine Technik zur Verwaltung der Anzahl der Verweise (Referenzen oder Zeiger) auf ein bestimmtes Objekt. Das Ziel ist dabei, zu erkennen, wann ein Objekt nicht mehr benötigt wird und gelöscht werden kann. Referenzzählung ist eine Möglichkeit zur automatischen Speicherbereinigung.

Stack Canary: Sprachen wie C erlauben aufgrund ihres Designs nicht immer die Überprüfung der Feldgrenzen (Beispiel: gets). Die Compiler müssen andere Wege gehen: Sie fügen zwischen der Rücksprungadresse und den lokalen Variablen Platz für eine Zufallszahl (auch „Canary“ genannt) ein. Beim Programmstart wird diese Zahl ermittelt, wobei sie jedes Mal unterschiedliche Werte annimmt. Der erforderliche Code wird vom Compiler automatisch generiert. Vor dem Verlassen des Programms über die Rücksprungadresse fügt der Compiler Code ein, der die Zufallszahl auf den vorgesehenen Wert überprüft. Wurde sie geändert, ist auch der Rücksprungadresse nicht zu trauen. Das Programm wird mit einer entsprechenden Meldung abgebrochen. Bei jedem Unterprogrammaufruf wird die Zufallszahl in den dafür vorgesehenen Bereich geschrieben.