

## APPVISORY PrePentest **Corona-Warn-App (Android)**

**Durchschnitt CVSS 5.2 (medium)**

**Höchster CVSS 7.5 (high)**

### App-Informationen

- Hersteller Robert Koch-Institut
- Name Corona-Warn-App
- Betriebssystem Android
- Version 1.3.0
- Erscheinungsdatum 02.09.2020
- Bundle-Identifier de.rki.coronawarnapp
- Benötigte OS-Version Android 6.0 oder höher
- Store-Link <https://play.google.com/store/apps/details?id=de.rki.coronawarnapp&hl=de>
- Store-Kategorie Gesundheit und Fitness

# Inhaltsverzeichnis

1 Testergebnis.....	3
1.1 Zusätzliche Funktionalitäten.....	3
1.1.1 In-App-Käufe.....	3
1.1.2 Externe Cloud-Dienste.....	3
1.1.3 Externe Login-Dienste.....	3
1.1.4 Social Network Sharing.....	4
1.1.5 Verwendung Webviews.....	4
2 Durchgeführte Analysevektoren.....	4
3 Testergebnisse.....	4
3.1 Test Setup.....	4
3.2 Tracking-Dienste.....	5
3.3 Virenanalyse.....	5
3.4 Berechtigungsanalyse.....	5
3.5 Binärdatei-Analyse.....	6
3.6 Risikobewertung.....	8
3.6.1 Datenschutzverstöße.....	8
3.6.2 Datensicherheitsverstöße.....	8
4 Verbindungsanalyse.....	8
4.1 Analyse Serververbindungen.....	9
4.1.1 Auszug Datenübertragungsprotokoll.....	9
4.1.1.1 Etag und meta-cwa-hash an t-online.de.....	9
5 Summary.....	10

# 1 Testergebnis

Corona-Warn-App	Version 1.3.0	Android
<b>Datenschutzverstöße</b> <ul style="list-style-type: none"><li>kein Verstoß festgestellt.</li></ul>	Einstufung	<b>unbedenklich</b>
<b>Datensicherheitsverstöße</b> <ul style="list-style-type: none"><li>kein Verstoß festgestellt.</li></ul>	Einstufung	<b>unbedenklich</b>
<b>AGB und Datenschutzerklärung</b> <ul style="list-style-type: none"><li>Keine Überprüfung der Datenschutzerklärung vorgenommen</li></ul>	Einstufung	<b>nicht verfügbar</b>
<b>SSL/TLS Analyse</b> <ul style="list-style-type: none"><li>eine Man-In-The-Middle-Attacke war erfolgreich</li></ul>	Einstufung	<b>bedenklich</b>

## 1.1 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 Nutzer-Accounts über ein bereits bestehendes Profil eines sozialen Netzwerks.

### 1.1.1 In-App-Käufe

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

### 1.1.2 Externe Cloud-Dienste

Die Applikation ermöglicht keine Sicherung von Daten über externe Cloud-Dienste.

Über Cloud-Dienste ist es theoretisch möglich, firmeninterne und möglicherweise geheime, sicherheitsrelevante oder anderweitig schützenswerte Daten manuell oder automatisch auf fremde, unbekannte Server eines Drittanbieters zu übertragen. Die Serverstandorte können im Ausland liegen. Es besteht die Möglichkeit eines unkontrollierten Datenabflusses.

### 1.1.3 Externe Login-Dienste

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

### 1.1.4 Social Network Sharing

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

### 1.1.5 Verwendung Webviews

Die Applikation verwendet keine Webviews.

## 2 Durchgeführte Analysevektoren

TLS analysierbar?	ja
-------------------	----

Sniffing Item	Kategorie	Übertragung festgestellt	Verschlüsselung
Etag	Metadata	ja	ja
meta-cwa-hash	Metadata	ja	ja

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

## 3 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 technische Dokumentation kann im Kapitel 4 eingesehen werden. Dort finden sich ausführliche Informationen über Datenverbindungen und Datentransfer.

### 3.1 Test Setup

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

- Testdatum 08. September 2020

- Testgerät Nexus 6P (Android 7.1.2)
- Testumgebung mediaTest digital Testlabor
- Prüfspezifikation mediaTest digital Prüfspezifikation rev. 2.0

### 3.2 Tracking-Dienste

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.

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

Tracker	Beschreibung
• Keine Funde	

### 3.3 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.

• Dateiname	Corona Warn App_v1.3.0.apk
• SHA256 Hashwert	e1546369ac15644b92d200bdc31905052eeddbaf88e9ce28216c8fb1411277cc
• Virensan-Ergebnis	<b>Funde: 0 von 63</b>

### 3.4 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 <b>nicht</b> 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.

Die Applikation fordert die folgenden Berechtigungen an.

Berechtigung	Beschreibung	Einstufung	Nutzung	Notwendig
Kamera	Erlaubt einer App den Zugriff auf die Kamera des Gerätes und die Möglichkeit Fotos und Videos aufzunehmen	• riskant	Ja	ja
Bluetooth	Erlaubt einer App den Zugriff auf die Bluetoothfunktion des Gerätes	• riskant	Ja	ja
Mitteilungen	Erlaubt einer App den Zugriff auf die Push-Mitteilungs Funktion.	• normal	Ja	ja

Die Berechtigungsanalyse zeigt die Verwendung von **3** 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 nicht als überprivilegiert eingestuft.

### 3.5 Binärdatei-Analyse

Problematik	Schweregrad	Standards	Beschreibung
App uses SQLite Database and execute raw SQL query.	High	<b>CVSS V2:</b> 5.9 (medium)  <b>CWE:</b> CWE-89 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') <b>OWASP Top 10:</b> M7: Client Code Quality	Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.
Insecure Implementation of SSL.	High	<b>CVSS V2:</b> 7.4 (high) <b>CWE:</b> CWE-295 - Improper Certificate Validation <b>OWASP Top 10:</b> M3: Insecure Communication <b>OWASP MASVS:</b> MSTG-NETWORK-3	Trusting all the certificates or accepting self signed certificates is a critical Security Hole. This application is vulnerable to MITM attacks
The App logs information.	Info	<b>CVSS V2:</b> 7.5 (high) <b>CWE:</b> CWE-532 - Insertion of Sensitive Information into Log File <b>OWASP MASVS:</b> MSTG-STORAGE-3	Sensitive information should never be logged.
This App uses Java Hash Code.	warning	<b>CVSS V2:</b> 2.3 (low) <b>CWE:</b> CWE-327 - Use of a Broken or Risky Cryptographic Algorithm <b>OWASP MASVS:</b> MSTG-CRYPTO-4	It's a weak hash function and should never be used in Secure Crypto Implementation.
This App uses SQL Cipher.	Info	<b>CVSS V2:</b> 0 (info) <b>OWASP MASVS:</b> MSTG-CRYPTO-1	SQLCipher provides 256-bit AES encryption to sqlite database files.

## 3.6 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.

### 3.6.1 Datenschutzverstöße

In diesem Unterkapitel werden die Datenschutzverstöße aufgelistet und eine Handlungsempfehlung abgegeben. Als Datenschutzverstoß wird die Übertragung eines personenbezogenen<sup>1</sup> oder anderweitig sensiblen Datums an Dritte definiert.

---

Keine Funde festgestellt

siehe - / -

**Handlungsempfehlung:**

### 3.6.2 Datensicherheitsverstöße

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

---

Keine Funde festgestellt

siehe - / -

**Handlungsempfehlung:**

---

**HINWEIS:**

---

**Handlungsempfehlung:** Kein Handlungsbedarf

---

## 4 Verbindungsanalyse

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

---

<sup>1</sup>



## 4.1 Analyse Serververbindungen

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

Nr.	Servername	IP-Adresse	Port	Land	Betreiber
V1	https://svc90.main.px.t-online.de	87.140.208.122	443	DE	T-Online

### 4.1.1 Auszug Datenübertragungsprotokoll

#### 4.1.1.1 Etag und meta-cwa-hash an t-online.de

```

Flow Details
https://svc90.main.px.t-online.de/version/v1/configuration/country/DE/app_config
2020-09-09 09:20:43 GET HTTP/1.1 ← 200 application/octet-stream 561b 65ms

Request Response Detail
Server: nginx
Date: Wed, 09 Sep 2020 07:20:43 GMT
Content-Type: application/octet-stream
Content-Length: 561
Connection: keep-alive
Etag: "5b8e94bfff5f525a558a75bae5436b6ae"
Last-Modified: Thu, 02 Jul 2020 09:05:15 GMT
Cache-Control: public,max-age=300
X-Header-Meta-Cwa-Hash: jao6c6b1a08910f1a861109b91a0da
Content-Security-Policy: default-src 'self' *.coronawarn.app; img-src 'self' *.coronawarn.app data;
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-XSS-Protection: 1
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Accept-Ranges: bytes

Hex
00000000 50 4b 03 04 14 08 08 08 08 a7 48 e2 50 00 00 PK.....H.P...
00000001 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ex
00000002 70 6f 72 74 2e 02 69 6e e3 e0 16 f2 e5 52 e6 62 port.bin....R.b
00000003 06 f1 0f 97 e0 57 92 ca 28 29 29 28 b0 d2 d7 2f ....M...().../
00000004 2f 2f 07 4b ce 2f ca cf 4b 2c 4f 2c ca d3 4b 2c //K//..K.O...K
00000005 28 e0 52 43 02 f1 f0 74 77 10 e0 97 f0 c0 a7 4e (R.b...E...W
00000006 2a 85 4b 80 83 51 80 49 82 59 81 45 83 d5 80 cd *.K..Q.I.Y.E...
00000007 82 dd 81 43 90 01 0c 3c 1d a4 b8 14 18 35 18 8d ...C...<...5...
00000008 18 2d 18 1d 18 15 01 82 5a 02 1c ac 02 ac 12 ac ...a.Z...
00000009 03 ac 40 f5 ac 16 ac 0e ac 00 10 29 15 07 20 30 @.....)....P
0000000a 01 46 09 46 84 16 47 98 1e 25 19 2e 10 0e 73 81 .F.F..G..N...s.
0000000b 7b 21 21 4e 88 d0 07 7b a8 25 0f ec 15 24 b5 a4 {[I.N...{N...S...
0000000c b8 08 08 08 08 38 24 98 84 08 04 58 85 78 80 6a ...X.B5...X.x.J
0000000d 19 25 58 04 c0 24 00 50 4b 07 00 df 2c 78 8d af *.K..$.PK...x...
0000000e 00 00 00 f1 00 00 00 50 4b 03 04 14 00 08 08 88 .....PK.....
0000000f 00 a7 48 e2 50 00 00 00 00 00 00 00 00 00 00 00 ..H.P.....
00000100 00 00 00 00 05 70 70 6f 72 74 2e 73 69 67 01 ....export.sig.
00000101 07 00 7f 0a 84 01 0a 34 0a 14 64 65 2e 72 60 ...X...d..de.rk
00000102 69 2e 63 6f 72 6f 6e 61 77 61 72 0e 61 70 70 1a t.coronawarnapp.
00000103 02 76 31 22 03 32 36 32 2a 13 31 2e 32 2e 38 34 .v1".262*.1.2.84
00000104 30 2e 31 30 30 34 35 2e 34 2e 33 2e 32 10 01 18 0.10045.4.3.2...
00000105 01 22 48 30 46 02 21 00 0c 31 79 55 35 4c f3 02 "HMF...1.yj05L...
00000106 ab 2f 38 2a ef 4a 7d 8f eb 02 76 4b af 38 cc 57 /8*.J)...vK.S.W
00000107 24 05 d6 0c 9c c2 43 2d 02 21 00 c3 2b 34 a2 a0 S....C..1..+4...
00000108 7d c9 01 aa bd 34 95 39 f5 25 da 71 89 a0 3f ]....4.9.K.q.??
00000109 ab f5 e0 73 85 73 f0 ed 01 c0 fc 58 4b 07 08 ac ...s....PK...
0000010a 9e 82 dd 8c 00 00 87 00 00 00 50 4b 01 02 14 .....PK...
0000010b 00 14 00 08 08 08 00 a7 48 e2 50 df 2c 78 8d af .....H.P.x...
0000010c 00 00 f1 00 00 0a 00 00 00 00 00 00 00 00 00 .....
0000010d 00 00 00 00 00 00 00 00 05 70 6f 72 74 2e .....export.
0000010e 02 69 6e 58 4b 01 02 14 00 14 00 08 08 00 a7 binPK.....
0000010f 48 e2 50 ac 9e 82 dd 8c 00 00 00 87 00 00 00 0a H.P.....
00000200 00 00 00 00 00 00 00 00 00 00 00 00 e7 00 00 .....
00000210 00 05 70 6f 72 74 2e 73 69 67 50 4b 65 00 00 .....export:slgPK...
00000220 00 00 02 00 02 00 70 00 00 00 ab 01 00 00 00 .....p.....
00000230 00

```

Abbildung 1.1 Etag und meta-cwa-hash werden an t-online.de übertragen

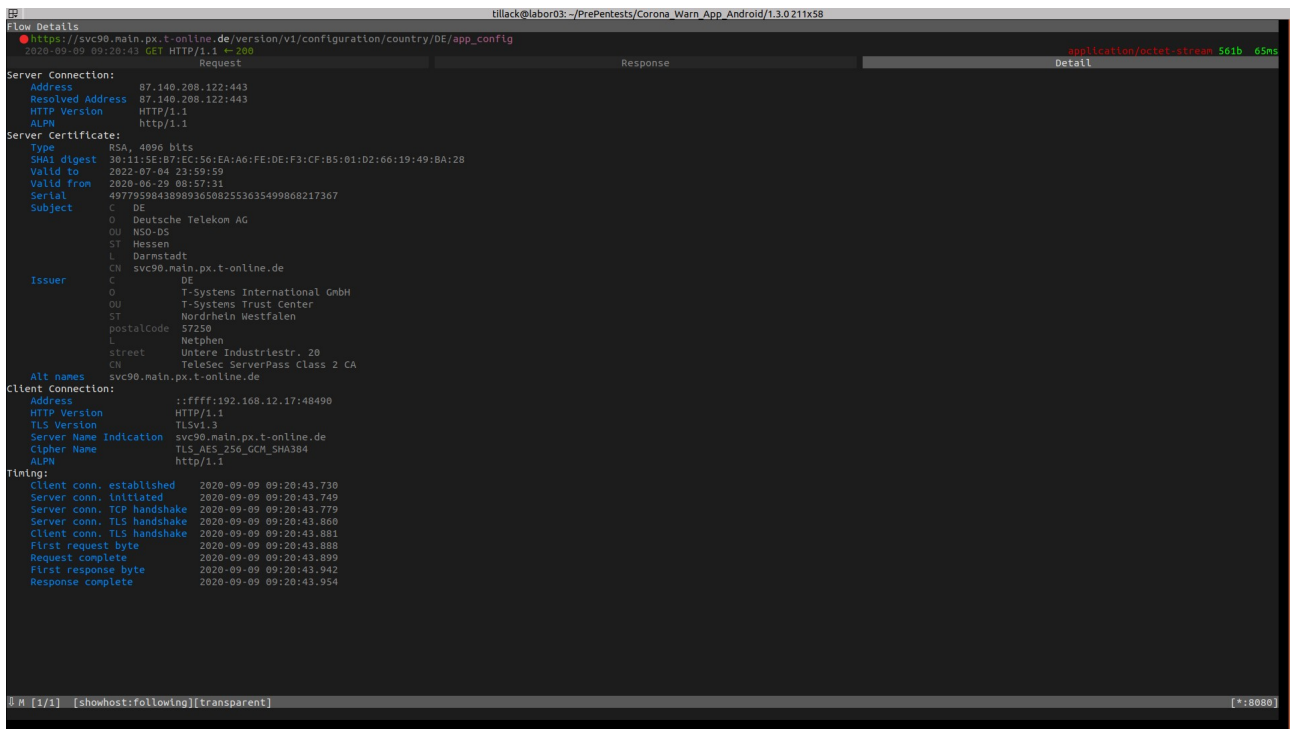


Abbildung 1.2 Server-Details t-online.de

## 5 Summary

Die Nutzung von Trackern oder Analyse-Tools konnte nicht festgestellt werden. Die Root-detection ist rudimentär implementiert. Gesammelte Daten werden möglicherweise nur lokal verarbeitet, da die volle Funktionsweise der Applikation uns während des Testlaufes nicht zur Verfügung stand (QR-Code). Es ist nicht absehbar was mit den gespeicherten Daten passiert, da die Kernfunktion der Applikation von dem jeweiligen Systemhersteller (Apple und Google) zur Verfügung gestellt wird.