



APPVISORY PrePentest **Corona-Warn-App (iOS)**

Durchschnitt CVSS 4.0 (medium)

Höchster CVSS 6.0 (medium)

App-Informationen

- Hersteller Robert Koch-Institut
- Name Corona-Warn-App
- Betriebssystem iOS
- Version 1.3.0
- Erscheinungsdatum 04.09.2020
- Bundle-Identifier de.rki.coronawarnapp
- Benötigte OS-Version iOS 13.5 oder höher
- Store-Link <https://apps.apple.com/de/app/corona-warn-app/id1512595757>
- 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.....	7
3.6.1 Datenschutzverstöße.....	8
3.6.2 Datensicherheitsverstöße.....	8
4 Verbindungsanalyse.....	8
4.1 Analyse Serververbindungen.....	8
4.1.1 Auszug Datenübertragungsprotokoll.....	9
4.1.1.1 Etag und meta-cwa-hash an t-online.de.....	9
5 Mitigationstechniken.....	10
6 Summary.....	10

1 Testergebnis

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

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 09. September 2020

- Testgerät iPhone 7 (iOS 13.5.1)
- 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	de.rki.coronawarnapp.ipa
• SHA256 Hashwert	ee80f8a34ac94eed46d0996ed09e324cfb989cfcb8801838b337ec49cc8d70c3
• Virensan-Ergebnis	Funde: 0 von 61

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 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.

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
-------------	-------------	-----------	--------------

Binary make use of insecure API(s)	High	CVSS V2: 6 (medium) CWE: CWE-676 - Use of Potentially Dangerous Function OWASP Top 10: M7: Client Code Quality OWASP MASVS: MSTG-CODE-8	The binary may contain the following insecure API(s) <code>_fopen</code> , <code>_memcpy</code> , <code>_strlen</code> .
Binary make use of malloc function	High	CVSS V2: 2 (low) CWE: CWE-789 - Uncontrolled Memory Allocation OWASP Top 10: M7: Client Code Quality OWASP MASVS: MSTG-CODE-8	The binary may use <code>_malloc</code> function instead of <code>calloc</code> .
Binary make use of Logging function	Info	CVSS V2: 7.5 (high) CWE: CWE-532 - Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	The binary may use <code>_NSLog</code> function for logging.

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 personenbezogenen¹ 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.

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

¹

4.1.1 Auszug Datenübertragungsprotokoll

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

```
tilk@labor03:~/PrePentests/Corona_Warn_App_ios/1.3.0.211x58
Flow Details
https://svc90.main.px.t-online.de/version/v1/configuration/country/DE/app_config
2020-09-09 09:40:33 GET HTTP/1.1 ← 200 application/octet-stream 561b 70ms
Request Response Detail
Server: nginx
Date: Wed, 09 Sep 2020 07:40:33 GMT
Content-Type: application/octet-stream
Content-Length: 501
Connection: keep-alive
Etag: "5b8e9dbff5f525a58a75bae5436b6ae"
Last-Modified: Thu, 02 Jul 2020 09:05:15 GMT
Cache-Control: public,max-age=3600
X-meta-cwa-hash: 13ced0b164059161a061109b91a0da
Content-Security-Policy: default-src 'self' *.coronawarn.app; img-src 'self' *.coronawarn.app data;
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 00 08 08 00 00 a7 48 e2 50 00 00 PK.....H.P...
00000001 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 65 78 .....ex
00000002 70 6f 72 74 2e 62 69 6e e3 e0 16 f2 e5 52 e6 62 port.bin....R.b
00000003 f6 f1 0f 97 e6 57 92 ca 28 29 29 28 b6 d0 67 2f .....M.().-./
00000004 2f 2f d7 4b ce 2f ca cf 4b 2c 4f 2c ca d3 4b 5c //K//kX0...K
00000005 28 e0 52 e3 e2 f1 f0 74 f7 10 e0 97 f0 c0 a7 4e (.R.b.t.....N
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 01 43 98 01 0c 2c 1d 04 00 14 18 35 18 00 ...C...S...S...
00000008 18 2d 1d 18 15 61 82 5a 02 1c ac 02 ac 12 ac .....S...S...
00000009 0a ac 40 f5 ac 16 ac 0e ac 86 10 29 13 07 2b 3e ..g.....)+>
0000000a 01 46 09 46 84 1e 47 98 1e 25 19 2e 10 0e 73 01 .F.F.G.K...S.
0000000b f0 21 4e 8b 00 07 7b 4b 25 0f ee 15 24 b5 04 [11W...[K...S-
0000000c b8 b8 b8 58 04 38 24 98 04 98 04 58 85 78 80 6a ...X.SS...X.X.J
0000000d 19 25 58 04 c0 24 00 50 4b 07 08 df 2c 78 8d af ..X..S.PK...X..
0000000e 00 00 f1 00 00 00 50 4b 03 04 14 00 08 08 00 .....PK.....
0000000f 00 07 48 e2 50 00 00 00 00 00 00 00 00 00 00 00 .....H.P.....
00000010 00 00 00 00 65 78 60 6f 72 74 2e 73 60 67 01 .....export.sig
00000011 07 00 78 ff 0a 04 01 0a 34 0a 14 64 65 2e 72 6b ...x....4..de.rk
00000012 09 2e 63 6f 72 6f 6e 61 77 01 72 6e 61 70 70 1a t.coronawarnapp.
00000013 02 70 22 03 32 30 32 2a 13 2e 32 2e 38 34 ..v1.2020.1.2.84
00000014 30 2e 31 30 30 34 05 6f 14 2e 33 2e 30 01 18 0.10045-4-3-2...
00000015 01 22 48 30 46 02 21 00 dc 31 79 55 35 4c f3 b2 ..HBF.I..lyUSL...
00000016 ab 2f 38 2a ef 4a 7d 8f eb 02 76 4b af 38 cc 57 ./B*.J)...vk.8.W
00000017 04 05 0c 0c 9c cd 43 2d 02 21 00 34 a2 60 $....C...l...+...
00000018 7d 69 01 aa b2 60 34 95 99 f5 25 7a 70 80 3f ]...-d.S.k.Q.-2
00000019 ab f5 e0 73 85 73 f9 ed b1 c6 fc 50 4b 07 08 ac ...S.S...PK...
0000001a 9e 82 dd 8c 00 00 00 87 00 00 50 4b 01 02 14 .....PK...
0000001b 00 14 00 08 08 00 a7 48 e2 50 df 2c 78 8d af .....H.P...X...
0000001c 00 00 00 00 6a 00 00 00 00 00 00 00 e7 00 00 .....-...
0000001d 00 00 00 00 00 00 00 00 65 78 70 6f 72 74 2e .....export.
0000001e 02 69 6e 50 4b 01 02 14 00 14 00 08 08 00 a7 binPK.....
0000001f 48 e2 50 ac 9e 82 dd 8c 00 00 87 00 00 00 0a H.P.....
00000020 00 00 00 00 00 00 00 00 00 00 00 00 e7 00 00 .....-...
00000021 00 65 78 70 6f 72 74 2e 73 69 67 50 4b 05 06 00 ..export.sigPK...
00000022 00 00 02 00 02 00 00 00 00 00 ab 01 00 00 00 .....p.....
00000023 00
[25/25] [showhost][transparent] [*:8080]
```

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

```
tilk@labor03:~/PrePentests/Corona_Warn_App_ios/1.3.0.211x58
Flow Details
https://svc90.main.px.t-online.de/version/v1/configuration/country/DE/app_config
2020-09-09 09:40:33 GET HTTP/1.1 ← 200 application/octet-stream 561b 70ms
Request Response Detail
Server Connection:
Address: 87.140.208.122:443
Resolved Address: 87.140.208.122:443
HTTP Version: HTTP/1.1
ALPN: http/1.1
Server Certificate:
Type: RSA, 4096 bits
SHA1 digest: 30:11:5E:B7:EC:56:EA:A6:FE:DE:F3:CF:B5:01:D2:66:19:49:BA:28
Valid to: 2022-07-04 23:59:59
Valid from: 2020-06-29 08:57:31
Serial: 497975943898935082553635499868217367
Subject:
C: DE
O: Deutsche Telekom AG
OU: NSO-DS
ST: Hessen
L: Darmstadt
CN: svc90.main.px.t-online.de
Issuer:
C: DE
O: T-Systems International GmbH
OU: T-Systems Trust Center
ST: Nordrhein Westfalen
postalCode: 57250
L: Netphen
street: Untere Industriest. 20
CN: Telesec ServerPass Class 2 CA
Client Connection:
Address: ::ffff:192.168.12.218:59822
HTTP Version: HTTP/1.1
TLS Version: TLSv1.3
Server Name Indication: svc90.main.px.t-online.de
Cipher Name: TLS_AES_256_GCM_SHA384
ALPN: http/1.1
Timing:
Client conn. established: 2020-09-09 09:40:25.991
Server conn. initiated: 2020-09-09 09:40:26.002
Server conn. TCP handshake: 2020-09-09 09:40:26.027
Server conn. TLS handshake: 2020-09-09 09:40:26.120
Client conn. TLS handshake: 2020-09-09 09:40:26.142
First request byte: 2020-09-09 09:40:33.268
Request complete: 2020-09-09 09:40:33.275
First response byte: 2020-09-09 09:40:33.322
Response complete: 2020-09-09 09:40:33.338
[25/25] [showhost][transparent] [*:8080]
```

Abbildung 1.2 Server-Details t-online.de

5 Mitigationstechniken

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

Position-independent-Executable	Enabled
---------------------------------	----------------

Eine Position-independent-Executable (PIE) 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	Enabled
------------------------------	----------------

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	Enabled
--------------	----------------

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.

6 Summary

Die Nutzung von Trackern oder Analyse-Tools konnte nicht festgestellt werden. Die Jailbreak-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.