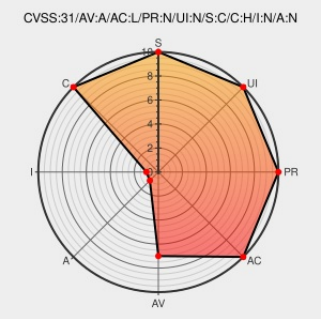
CVE-2020-26230

Published on: 11/13/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:56 PM UTC

CVE-2020-26230 - advisory for GHSA-w7jx-37x3-w2jx

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Radar-covid-backend-dp3t-server from Radarcovid contain the following vulnerability:

Radar COVID is the official COVID-19 exposure notification app for Spain. In affected versions of Radar COVID, identification and de-anonymization of COVID-19 positive users that upload Radar COVID TEKs to the Radar COVID server is possible. This vulnerability enables the identification and de-anonymization of COVID-19 positive users when using Radar COVID. The vulnerability is caused by the fact that Radar COVID connections to the server (uploading of TEKs to the backend) are only made by COVID-19 positives. Therefore, any on-path observer with the ability to monitor traffic between the app and the server can identify which users had a positive test. Such an adversary can be the mobile network operator (MNO) if the connection is done through a mobile network, the Internet Service Provider (ISP) if the connection is done through the Internet (e.g., a home network), a VPN provider used by the user, the local network operator in the case of enterprise networks, or any eavesdropper with access to the same network (WiFi or Ethernet) as the user as could be the case of public WiFi hotspots deployed at shopping centers, airports, hotels, and coffee shops. The attacker may also de-anonymize the user. For this additional stage to succeed, the adversary needs to correlate Radar COVID traffic to other identifiable information from the victim. This could be achieved by associating the connection to a contract with the name of the victim or by associating Radar COVID traffic to other user-generated flows containing identifiers in the clear (e.g., HTTP cookies or other mobile flows sending unique identifiers like the IMEI or the AAID without encryption). The former can be executed, for instance, by the Internet Service Provider or the MNO. The latter can be executed by any on-path adversary, such as the network provider or even the cloud provider that hosts more than one service accessed by the victim. The farther the adversary is either from the victim (the client) or the end-point (the server), the less likely it may be that the adversary has access to re-identification information. The vulnerability has been mitigated with the injection of dummy traffic from the application to the backend. Dummy traffic is generated by all users independently of whether they are COVID-19 positive or not. The issue was fixed in iOS in version 1.0.8 (uniform distribution), 1.1.0 (exponential distribution), Android in version 1.0.7 (uniform distribution), 1.1.0 (exponential distribution), Backend in version 1.1.2-RELEASE. For more information see the referenced GitHub Security Advisory.

CVE-2020-26230 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **RadarCOVID** - **radar-covid-backend-dp3t-server** version **iOS version < 1.0.8**

Affected Vendor/Software: **RadarCOVID** - **radar-covid-backend-dp3t-server** version **Android version < 1.0.7**

Affected Vendor/Software: **RadarCOVID** - **radar-covid-backend-dp3t-server** version **Backend < 1.1.2-RELEASE**

CVSS3 Score: 5.3 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: 2.6 - LOW

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
chore: fix execution delay · RadarCOVID/radar-covid-android@7fdc7de · GitHub	Patch, Third Party Advisory, github.com, text/html	MISC github.com/RadarCOVID/radar-covid-android/commit/7fdc7debeb8a37faa77b53d9f9a1b4bbcff445ce
chore: fix build config import · RadarCOVID/radar-covid-android@09d00e5 · GitHub	Patch, Third Party Advisory, github.com, text/html	MISC github.com/RadarCOVID/radar-covid-android/commit/09d00e5ede801ca400d45c7feda5a99c34e4176c
*Added exponential interval for fake request · RadarCOVID/radar-covid-android@5325277 · GitHub	Patch, Third Party Advisory, github.com, text/html	MISC github.com/RadarCOVID/radar-covid-android/commit/53252773ffa81e116deabcbbea3bac96872b9888
chore: release 1.1.0 · RadarCOVID/radar-	Patch, Third Party Advisory	MISC github.com/RadarCOVID/radar-covid-ios/commit/2d1505d4858642995ea09f02f23c953acaa65195

covid-ios@2d1505d · GitHub	github.com text/html	
documents/DP3T - Best Practices for Operation Security in Proximity Tracing.pdf at master · DP-3T/documents · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/DP-3T/documents/blob/master/DP3T%20-%20Best%20Practices%20for%20Operation%20Security%20in%20Proximity%20Tracing.pdf
[MAPR] AOP aspects ordering · RadarCOVID/radar-covid-backend-dp3t-server@6d30c92 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/RadarCOVID/radar-covid-backend-dp3t-server/commit/6d30c92cc8fcbde3ded7e9518853ef278080344d
chore: Changed ExistingWorkPolicy to REPLACE in fake request worker · RadarCOVID/radar-covid-android@9627f4d · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/RadarCOVID/radar-covid-android/commit/9627f4d69705bca68e550eefd3df1b9abe90b215
Identification and deanonymization of COVID-19 positive users that upload Radar COVID TEKs to the Radar COVID server. · Advisory · RadarCOVID/radar-covid-backend-dp3t-server · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/RadarCOVID/radar-covid-backend-dp3t-server/security/advisories/GHSA-w7jx-37x3-w2jx
[MAPR] Setted responses retention time on fake requests · RadarCOVID/radar-covid-backend-dp3t-server@c37f816 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/RadarCOVID/radar-covid-backend-dp3t-server/commit/c37f816362508926707503989139fd76d4beffe
*[FakeReport] Implemented random fake infection reports · RadarCOVID/radar-covid-android@91dcfff · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/RadarCOVID/radar-covid-android/commit/91dcfff6252055637bc9ee0c46b8f003d64a16b9
*changed minutes for milliseconds · RadarCOVID/radar-covid-android@ea0c4cc · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/RadarCOVID/radar-covid-android/commit/ea0c4cc837f72f58e2b5df1ecf0899743ec3cdf8
*Code fix · RadarCOVID/radar-covid-android@8e5d14e · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/RadarCOVID/radar-covid-android/commit/8e5d14ec60e0c1847a4733556cf34d232c27102c

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Radarcovid	Radar-covid-backend-dp3t-server	All	All	All	All
Application	Radarcovid	Radar-covid-backend-dp3t-server	All	All	All	All
Application	Radarcovid	Radarcovid	All	All	exponential_distribution	All
Application	Radarcovid	Radarcovid	All	All	exponential_distribution	All
Application	Radarcovid	Radarcovid	All	All	uniform_distribution	All
Application	Radarcovid	Radarcovid	All	All	uniform_distribution	All
Application	Radarcovid	Radarcovid	All	All	exponential_distribution	All
Application	Radarcovid	Radarcovid	All	All	exponential_distribution	All
Application	Radarcovid	Radarcovid	All	All	uniform_distribution	All
Application	Radarcovid	Radarcovid	All	All	uniform_distribution	All

cpe:2.3:a:radarcovid:radar-covid-backend-dp3t-server:*:*:*:*:*:*:*:*:

cpe:2.3:a:radarcovid:radar-covid-backend-dp3t-server:*:*:*:*:*:*:*:*:

cpe:2.3:a:radarcovid:radarcovid:*:*:exponential_distribution:*:*:android:*:*:

cpe:2.3:a:radarcovid:radarcovid:*:*:exponential_distribution:*:*:iphone_os:*:*:

cpe:2.3:a:radarcovid:radarcovid:*:*:uniform_distribution:*:*:android:*:*:

cpe:2.3:a:radarcovid:radarcovid:*:*:uniform_distribution:*:*:iphone_os:*:*:

cpe:2.3:a:radarcovid:radarcovid:*:*:exponential_distribution:*:*:android:*:*:

cpe:2.3:a:radarcovid:radarcovid:*:*:exponential_distribution:*:*:iphone_os:*:*:

cpe:2.3:a:radarcovid:radarcovid:*:*:uniform_distribution:*:*:android:*:*:

cpe:2.3:a:radarcovid:radarcovid:*:*:uniform_distribution:*:*:iphone_os:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report