

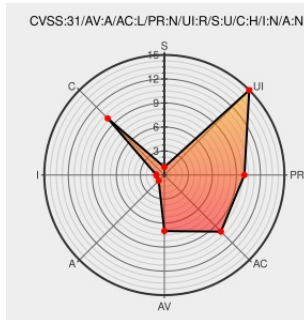


CVE-2020-14292

Published on: 09/09/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-14292

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Covidsafe](#) from [Health](#) contain the following vulnerability:

In the COVIDSafe application through 1.0.21 for Android, unsafe use of the Bluetooth transport option in the GATT connection allows attackers to trick the application into establishing a connection over Bluetooth BR/EDR transport, which reveals the public Bluetooth address of the victim's phone without authorisation, bypassing the Bluetooth address randomisation protection in the user's phone.

CVE-2020-14292 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.7 - MEDIUM**

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

CVSS2 Score: **2.9 - LOW**

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
GitHub - alwentiu/CVE-2020-14292: Details of CVE-2020-14292	Exploit Third Party Advisory	github.com/alwentiu/CVE-2020-14292

github.com
text/html

COVIDSafe app | Australian Government
Department of Health

Product
Third Party Advisory
www.health.gov.au
text/html

MISC www.health.gov.au/resources/apps-and-tools/covidsafe-app

COVIDSafe.watch - Issue Register

Vendor Advisory
covidsafe.watch
text/html

MISC covidsafe.watch/issue-register/

mobile-android/Work.kt at
b827cf3cccf72a3d38c6fc37466a99868823540f
· AU-COVIDSafe/mobile-android · GitHub

Exploit
Third Party Advisory
github.com
text/html

MISC github.com/AU-COVIDSafe/mobile-android/blob/b827cf3cccf72a3d38c6fc37466a99868823540f/app/src/main/java/au/covid19/mobile/android/Work.kt

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

Exploit/POC from Github

Details of CVE-2020-14292

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Health	Covidsafe	All	All	All	All
cpe:2.3:a:health:covidsafe:*:*:*:*:android:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)