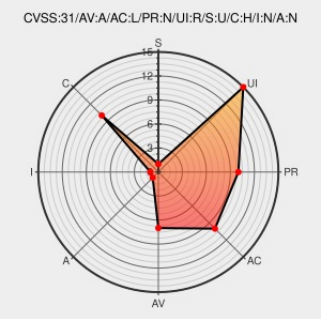
CVE-2020-14292

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 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	MISC 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 b827cf3ccef72a3d38c6fc37466a99868823540f · AU-COVIDSafe/mobile-android · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/AU-COVIDSafe/mobile-android/blob/b827cf3ccef72a3d38c6fc37466a99868823540f/app/src/m L41

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→