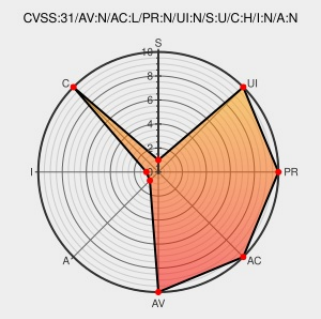
CVE-2020-12857

Published on: 05/18/2020 12:00:00 AM UTC

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

CVE-2020-12857

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



Certain versions of Covidsafe from Health contain the following vulnerability:

Caching of GATT characteristic values (TempID) in COVIDSafe v1.0.15 and v1.0.16 allows a remote attacker to long-term re-identify an Android device running COVIDSafe.

CVE-2020-12857 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
COVIDSafe app | Australian Government Department of Health	Product, Vendor Advisory, www.health.gov.au, text/html	MISC www.health.gov.au/resources/apps-and-tools/covidsafe-app

COVIDSafe.watch - CVE-2020-12857 - TempID identifier was static	Third Party Advisory covidsafe.watch text/html	MISC covidsafe.watch/issue-register/cve-2020-12857-tempid-identifier-was-static
COVIDSafe Android App - BLE Privacy Issues - Google Docs	Third Party Advisory docs.google.com text/html	MISC docs.google.com/document/d/1u5a5ersKBH6eG362atALrzuXo3zuZ70qrGomWVEC27U/edit?usp=sharing

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Health	Covidsafe	All	All	All	All
Application	Health	Covidsafe	All	All	All	All

cpe:2.3:a:health:covidsafe:*:*:*:*:*:android:*:*:

cpe:2.3:a:health:covidsafe:*:*:*:*:*:android:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→