

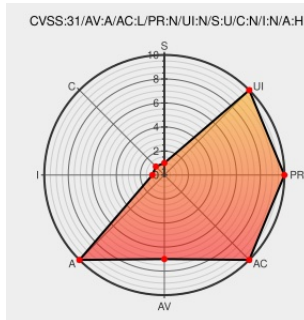


CVE-2020-12717

Published on: 05/14/2020 12:00:00 AM UTC

Last Modified on: 11/07/2023 03:15:00 AM UTC

CVE-2020-12717

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

Certain versions of [Abtracetgether](#) from [Alberta](#) contain the following vulnerability:

The COVIDSafe (Australia) app 1.0 and 1.1 for iOS allows a remote attacker to crash the app, and consequently interfere with COVID-19 contact tracing, via a Bluetooth advertisement containing manufacturer data that is too short. This occurs because of an erroneous OpenTrace manuData.subdata call. The ABTraceTogether (Alberta), ProteGO (Poland), and TraceTogether (Singapore) apps were also affected.

CVE-2020-12717 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **3.3 - LOW**

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

CVE References

Description	Tags	Link
COVIDSafe iOS Vulnerability — CVE-2020-12717 - Richard Nelson - Medium	medium.com text/html	MISC medium.com/@wabz/covidsafe-ios-vulnerability-cve-2020-12717-30dc003f9708

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

Code for exploit for CVE-2020-12717

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Alberta	Abtracetoegether	-	All	All	All
Application	Alberta	Abtracetoegether	-	All	All	All
Application	Gov	Protego Safe	-	All	All	All
Application	Gov	Protego Safe	-	All	All	All
Application	Health	Covidsafe	1.0	All	All	All
Application	Health	Covidsafe	1.1	All	All	All
Application	Health	Covidsafe	1.0	All	All	All
Application	Health	Covidsafe	1.1	All	All	All
Application	Tracetoegether	Tracetoegether	-	All	All	All
Application	Tracetoegether	Tracetoegether	-	All	All	All

cpe:2.3:a:alberta:abtracetoegether:-:*:*:*:iphone_os:*:*:

cpe:2.3:a:alberta:abtracetoegether:-:*:*:*:iphone_os:*:*:

cpe:2.3:a:gov:protego_safe:-:*:*:*:iphone_os:*:*:

cpe:2.3:a:gov:protego_safe:-:*:*:*:iphone_os:*:*:

cpe:2.3:a:health:covidsafe:1.0:*:*:*:iphone_os:*:*:

cpe:2.3:a:health:covidsafe:1.1:*:*:*:iphone_os:*:*:

cpe:2.3:a:health:covidsafe:1.0:*:*:*:iphone_os:*:*:

cpe:2.3:a:health:covidsafe:1.1:*:*:*:iphone_os:*:*:

cpe:2.3:a:tracetoegether:tracetoegether:-:*:*:*:iphone_os:*:*:

cpe:2.3:a:tracetoegether:tracetoegether:-:*:*:*:iphone_os:*:*:

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
← 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](#)