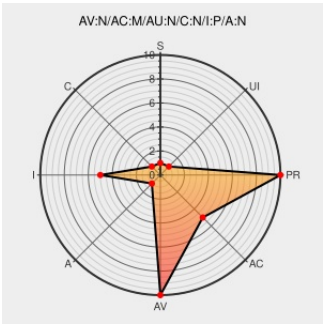
CVE-2014-7922

Published on: 02/22/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:49 PM UTC

CVE-2014-7922

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



Certain versions of Play Services Sdk from Google contain the following vulnerability:

The GoogleAuthUtil.getToken method in the Google Play services SDK before 2015 sets parameters in OAuth token requests upon finding a corresponding _opt_ parameter in the Bundle extras argument, which allows attackers to bypass an intended consent dialog and retrieve tokens for arbitrary OAuth scopes including the SID and LSID scopes, and consequently obtain access to a Google account, via a crafted application, as demonstrated by setting the has_permission=1 parameter value upon finding _opt_has_permission in that argument.

CVE-2014-7922 has been assigned by security@google.com to track the vulnerability

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
PoC for Android GoogleAuthUtil.getToken() bug · GitHub	Exploit, gist.github.com, text/html	MISC gist.github.com/isciurus/df4d7edd9c3efb4a0753
Untilted blog: Android app with full control over your Google account	Exploit, isciurus.blogspot.com, text/html	MISC isciurus.blogspot.com/2015/01/android-app-with-full-control-over-your.html

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	Google	Play Services Sdk	All	All	All	All

cpe:2.3:a:google:play_services_sdk:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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