

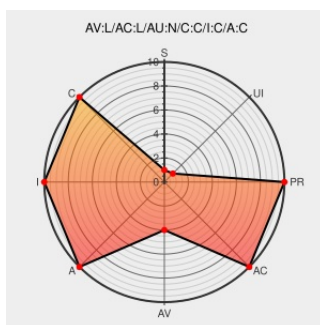


CVE-2011-1149

Published on: 04/21/2011 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:16 PM UTC

CVE-2011-1149

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

Certain versions of [Android](#) from [Google](#) contain the following vulnerability:

Android before 2.3 does not properly restrict access to the system property space, which allows local applications to bypass the application sandbox and gain privileges, as demonstrated by psneuter and KillingInTheNameOf, related to the use of Android shared memory (ashmem) and ASHMEM_SET_PROT_MASK.

CVE-2011-1149 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **7.2 - HIGH**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

No Description Provided

Patch

[android.git.kernel.org](#)



CONFIRM [android.git.kernel.org/?p=kernel/common.git;a=commit;h=c98a285075f26e2b17a5baa2cb3eb6356a75597e](#)

Inactive Link

Not Archived

No Description Provided

Patch

[android.git.kernel.org](#)



CONFIRM [android.git.kernel.org/?p=platform/system/core.git;a=commit;h=25b15be9120bcd00aba622c67ad2c835d9e91c](#)

Inactive Link

Not Archived

C skills: adb trickery
#2

[c-skills.blogspot.com](#)

[text/html](#)



MISC [c-skills.blogspot.com/2011/01/adb-trickery-again.html](#)

Google Groups

[groups.google.com](#)

[text/html](#)



CONFIRM [groups.google.com/group/android-security-discuss/browse_thread/thread/15f97658c88d6827/e86db04652651971?](#)

HTC Vision - XDA-Developers [Exploit](#) [forum.xda-developers.com](#) [text/html](#) [MISC forum.xda-developers.com/wiki/index.php?title=HTC_Vision#Rooting_the_G2](#)

text/html

scotty2 at scotty2 from
tmzt/g2root-kmod -
GitHub

text/html

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

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Google	Android	1.5	All	All	All
Operating System	Google	Android	1.6	All	All	All
Operating System	Google	Android	2.1	All	All	All
Operating System	Google	Android	2.2	rev1	All	All
Operating System	Google	Android	2.2.1	All	All	All
Operating System	Google	Android	1.5	All	All	All
Operating System	Google	Android	1.6	All	All	All
Operating System	Google	Android	2.1	All	All	All
Operating System	Google	Android	2.2	rev1	All	All
Operating System	Google	Android	2.2.1	All	All	All
Operating System	Google	Android	All	All	All	All

```
cpe:2.3:o:google:android:1.5:*:*:*:*:*:
```

cpe:2.3:o:google:android:1.6:*:*:*:*:*:

```
cpe:2.3:o:google:android:2.1:*:*:*:*:*
```

cpe:2.3:o:google:android:2.2:rev1:*.***.***:

cpe:2.3:o:google:android:2.2.1:*****:
cpe:2.3:o:google:android:1.5:*****:
cpe:2.3:o:google:android:1.6:*****:
cpe:2.3:o:google:android:2.1:*****:
cpe:2.3:o:google:android:2.2:rev1:*****:
cpe:2.3:o:google:android:2.2.1:*****:
cpe:2.3:o:google:android:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)