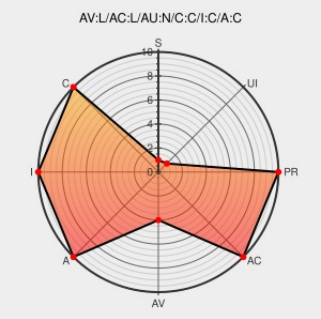
CVE-2011-1149

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	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
No Description Provided	Patch, android.git.kernel.org, Inactive Link, Not Archived	CONFIRM android.git.kernel.org/?p=kernel/common.git;a=commit;h=c98a285075f26e2b17a5baa2cb3eb6356a75597e
No Description Provided	Patch, android.git.kernel.org, Inactive Link, Not Archived	CONFIRM android.git.kernel.org/?p=platform/system/core.git;a=commit;h=25b15be9120bcdaa0aba622c67ad2c835d9e91c
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?

		show_docid=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
scotty2 at scotty2 from tmzt/g2root-kmod - GitHub	Patch github.com text/html	MISC github.com/tmzt/g2root-kmod/tree/scotty2/scotty2

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→