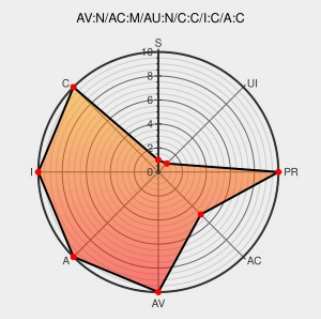
CVE-2011-3874

Published on: 01/27/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:13 PM UTC

CVE-2011-3874

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



Certain versions of Android from Google contain the following vulnerability:

Stack-based buffer overflow in libsysutils in Android 2.2.x through 2.2.2 and 2.3.x through 2.3.6 allows user-assisted remote attackers to execute arbitrary code via an application that calls the FrameworkListener::dispatchCommand method with the wrong number of arguments, as demonstrated by zergRush to trigger a use-after-free error.

CVE-2011-3874 has been assigned by security@google.com to track the vulnerability

CVSS2 Score: 9.3 - HIGH

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

CVE References

Description	Tags	Link
oss-security - Re: Re: CVE request: Android: vold stack buffer overflow	www.openwall.com text/html	MLIST [oss-security] 20111109 Re: Re: CVE request: Android: vold stack buffer overflow
zergRush/zergRush.c at master · revolutionary/zergRush · GitHub	Exploit github.com text/html	MISC github.com/revolutionary/zergRush/blob/master/zergRush.c
oss-security - Re: CVE request: Android: vold stack buffer overflow	www.openwall.com text/html	MLIST [oss-security] 20111108 Re: CVE request: Android: vold stack buffer overflow
Issue 21681 - android - CVE-2011-3874 - libsysutils rooting vulnerability ("zergRush") - Android Open Source Project - Issue Tracker - Google Project Hosting	Patch code.google.com text/html	CONFIRM code.google.com/p/android/issues/detail?id=21681

oss-security - CVE request: Android: vold stack buffer overflow	www.openwall.com text/html	MLIST [oss-security] 20111108 CVE request: Android: vold stack buffer overflow

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	2.2	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	2.2.2	All	All	All
Operating System	Google	Android	2.3	All	All	All
Operating System	Google	Android	2.3	rev1	All	All
Operating System	Google	Android	2.3.1	All	All	All
Operating System	Google	Android	2.3.2	All	All	All
Operating System	Google	Android	2.3.3	All	All	All
Operating System	Google	Android	2.3.4	All	All	All
Operating System	Google	Android	2.3.5	All	All	All
Operating System	Google	Android	2.3.6	All	All	All
Operating System	Google	Android	2.2	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	2.2.2	All	All	All
Operating System	Google	Android	2.3	All	All	All

Operating System	Google	Android	2.3	rev1	All	All
Operating System	Google	Android	2.3.1	All	All	All
Operating System	Google	Android	2.3.2	All	All	All
Operating System	Google	Android	2.3.3	All	All	All
Operating System	Google	Android	2.3.4	All	All	All
Operating System	Google	Android	2.3.5	All	All	All
Operating System	Google	Android	2.3.6	All	All	All

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

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

cpe:2.3:o:google:android:2.2.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:2.2.2:*:*:*:*:*:*:*:

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

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

cpe:2.3:o:google:android:2.3.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:2.3.2:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:2.3.3:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:2.3.4:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:2.3.5:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:2.3.6:*:*:*:*:*:*:*:

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

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

cpe:2.3:o:google:android:2.2.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:2.2.2:*:*:*:*:*:*:*:

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

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

cpe:2.3:o:google:android:2.3.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:2.3.2:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:2.3.3:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:2.3.4:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:2.3.5:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:2.3.6:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→